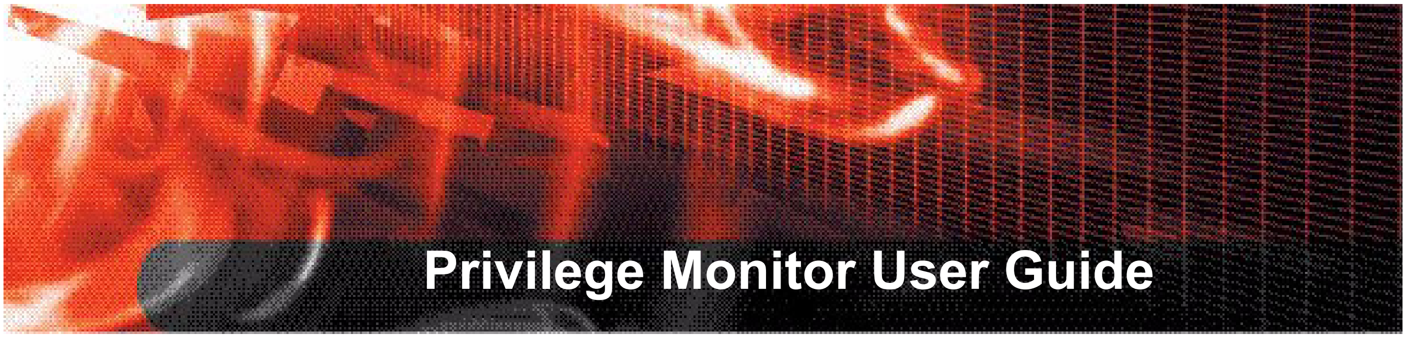


# Privilege Monitor User Guide

## FortiDB
## Version 3.2

FORTINET

www.fortinet.com

*FortiDB Privilege Monitor User Guide*
Version 3.2
December 19, 2008
15-32000-81364-20081219

**Trademarks**

# Table of Contents

# What is Privilege Monitor?

FortiDB MA Privilege Monitor (PM) examines, on a near real-time basis, privilege-setting changes in selected databases. For monitoring, you can specify the:

- Type of Item to monitor (System Views or User-Defined Rules (UDRs))
- Monitoring schedule, monitoring interval, or guard cycle
- Email recipients for violation alerts

PM also provides a:

- Privilege Summary feature by which you can see all the privileges currently assigned to your users, roles, and groups.
- UDR Results feature by which you can perform a quick test on your rules to see pre-existing and new violations.

# Steps to Use PM

Using PM generally involves these steps:

1 Logging in. For details about login, refer to the next section.

2 Creating a database connection. To create a database connection, refer to *Administration Guide.*

3 Connecting to your database. To connect to your database, refer to *Administration Guide*.

4 Setting a monitoring schedule To set a monitoring schedule, refer to Setting Schedules section.

5 (Optionally,) enabling email-report recipients. To enable email recipients, refer to Configuring Receivers for Alert Emails section.

6 (Optionally,) defining User-Defined Rules. To define UDR, refer to Adding or Creating a UDR section.

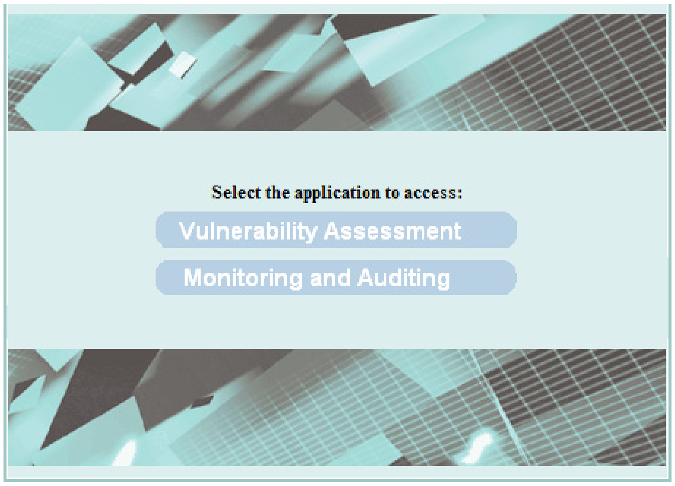
7 Specifying which System Views and/or rules to use for monitoring. To specify System View, refer to Setting Guarded Items section.

8 Activating Privilege Check. To activate Privilege check, refer to Activating Privilege Checking and Checking Status section.

9 Checking for alerts. To check alerts, refer to Analyzing Alerts section.

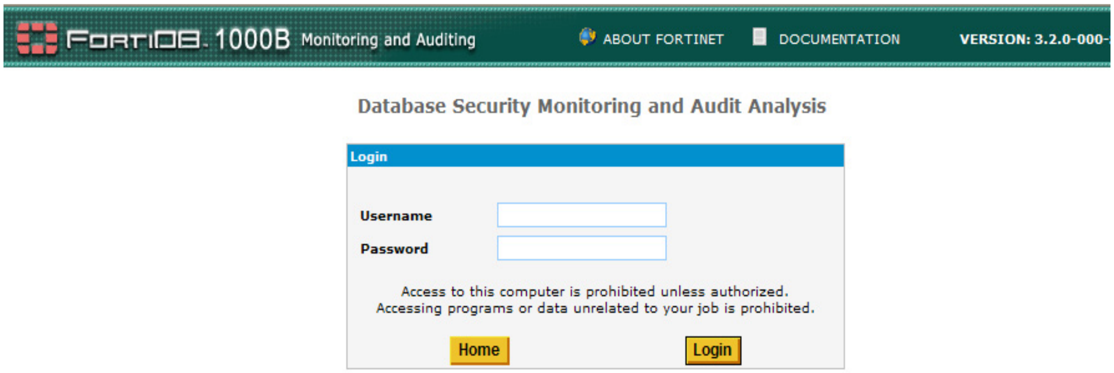
# Logging In

Open the FortiDB application in your browser. Depending upon its location with respect to your browser location and depending upon your chosen port number, that will require a specific URL.


Select the application to access:

From the FortiDB Main page, choose Monitoring and Auditing to access to FortiDB MA.

The FortiDB MA administrator is responsible for providing you with a username and an initial password. You can change your password after logging in.



Database Security Monitoring and Audit Analysis

Login

Username

Password

Access to this computer is prohibited unless authorized.
Accessing programs or data unrelated to your job is prohibited.

In order to login to Privilege Monitor, take the following steps:

**1** Enter your assigned user name.

**2** Enter your assigned password.

**3** Click the **Login** button. You will be presented with the application screen that gives access to the modules you are assigned.

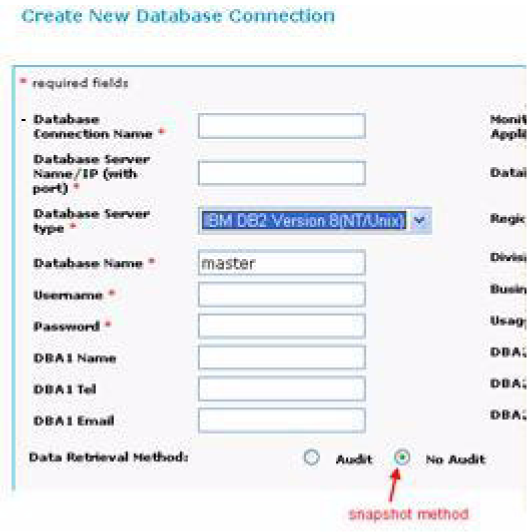
**4** Click the **Go** button on the Privilege Monitor line to proceed into the PM module.

By default, if you stop using PM for 30 minutes or more, you will need to login again in order to use the system. To modify this, please see information about `dss.sessionTimeout` in Appendix A: Property Files of the *FortiDB MA Administration Guide*.

**Note:** To go back to the FortiDB Main page, click the **Home** button. After login to Privilege Monitor, in order to go back to the FortiDB Main page, first you need to log out by clicking the **logout** link at the top bar. This brings you back to the login page. To display the FortiDB Main page, click the **Home** button.

# Audit vs. No Audit

Privilege Monitor offers No Audit (snapshot) method of data retrieval for all RDBMS types and an audit method for Oracle, DB2 UDB v8, and MS-SQL.



Create New Database Connection

* required fields

| | | |
|---|---|---|
| Database Connection Name * | | Monit Appli |
| Database Server Name/IP (with port) * | | Datal |
| Database Server type * | IBM DB2 Version 8(NT/Unix) | Regic |
| Database Name * | master | Divisi |
| Username * | | Busin |
| Password * | | Usag |
| DBA1 Name | | DBA: |
| DBA1 Tel | | DBA: |
| DBA1 Email | | DBA: |

Data Retrieval Method: ○ Audit ● No Audit

snapshot method

**Audit vs. No Audit (snapshot) Method of Data Retrieval**

## No Audit Method of Data Retrieval

No Audit (snapshot) method takes snapshots of system tables in order to alert you about any activity which results in changes to these tables. For this method, target-database access is limited to a defined interval or 'guard cycle'. Access within this interval is not captured by FortiDB MA and, consequently, does not generate alerts. For example, if you have configured a 1-minute monitoring interval, a privilege change that is made and undone within 59 seconds will not be captured and therefore cannot generate an alert.

Once you specify which items to monitor and at what frequency, Privilege Monitor scans your database and, using the monitoring interval you specify, writes snapshots of privilege settings to a log file. It then compares the current condition of those settings to previous snapshots in the file and reports on information such as:

- Rule violation
- Privilege change(s)
- Grantee
- Grantor
- Time of change

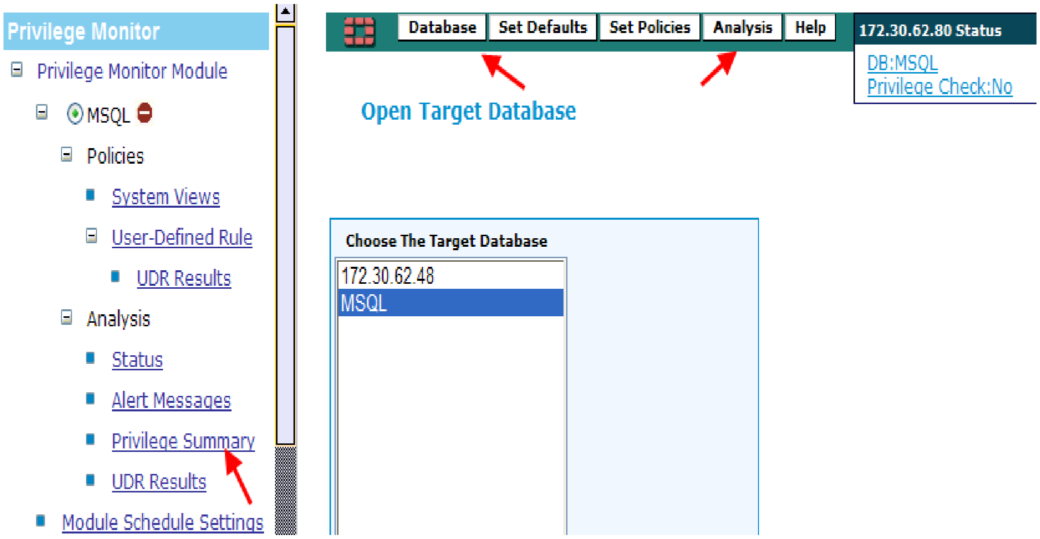
**Note:** If you close your database connection or get disconnected; e.g., because of a network outage, monitoring and reporting will stop. When you reconnect, the snapshot log from when you were last connected will be read and compared with current data and any changes made while you were offline will be noted.

## *The Audit Method of Data Retrieval*

The audit method relies upon audit records to generate alerts. Once auditing is set up for some event, *every* occurrence of the event is captured; the audit method results in information about all activities on the target database.

# Navigating Privilege Monitor

You can use Privilege Monitor via the Graphical User Interface (GUI), which is explained in this Guide, or via the command-line interface that is explained in the *FortiDB MA Command Line Interface (CLI) User Guide*.



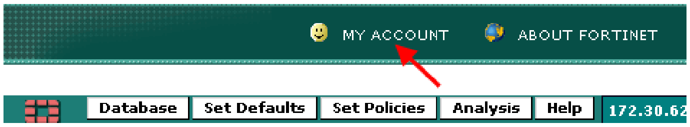
**Tree, Button, and Menu Navigation**

The GUI consists of two side-by-side windows:

- Located on the left side of the screen, you will a find hierarchical tree-style navigator.
- Located on the right side of the screen, you will find a menu-style navigator at the top with a button-style navigator below.

**Note:** In this manual, we will explain how to navigate primarily through the menu; however, you may find tree navigation and/or the buttons more convenient.

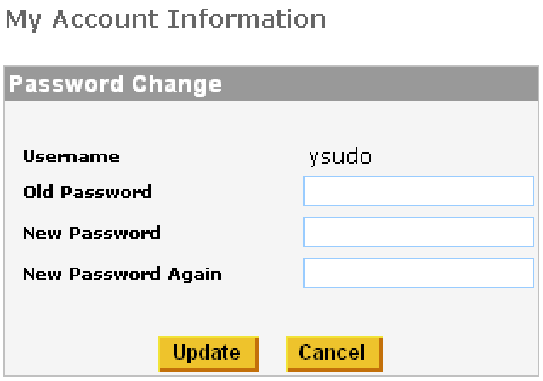
## Changing Your Password



**Navigating to the Password Change Dialog Box**

You can invoke the **Password Change** screen by clicking on the **MY ACCOUNT** tab at the top of the screen.

In order to change a password, you need to enter the **Old Password**, **New Password**, and **New Password Again**, and then click **Update**, for the password change to occur. If you change your mind, you may click **Cancel** to abort the process.



My Account Information

Password Change

Username ysudo

Old Password

New Password

New Password Again

**Figure 40: Password Change Dialog Box**

Please refer to the *Accoun and Password Management* in the *Administration Guide* for further information about User Administration.

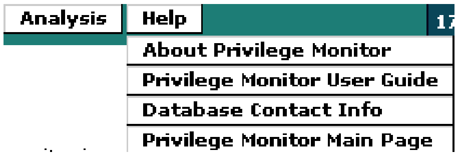
## ABOUT FortiDB MA Button

The **ABOUT** FortiDB MA button takes you to a web page with FortiDB MA contact information, including that for technical support. This button is on most FortiDB MA screens.

## DOCUMENTATION Button

The **DOCUMENTATION** button takes you to a page with links to the FortiDB MA documentation. This link is on most FortiDB MA screens.

## The PM Help Menu



**PM Help Menu**

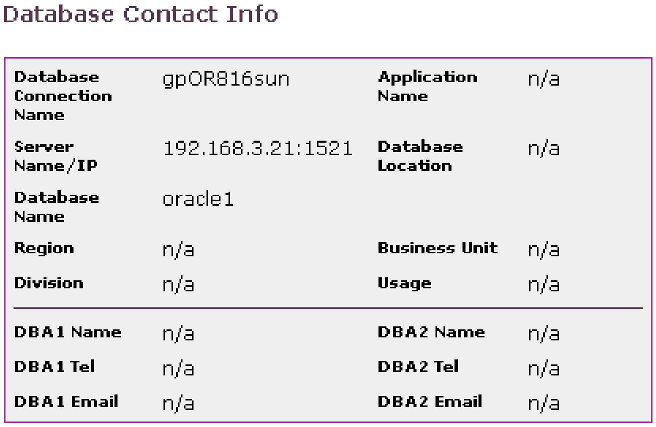
The PM Help Menu provides:

- Module version and build number inforation
- A link to the *PM User Guide*
- Connection-specific database information
- A link to get back to the initial PM screen

### About Privilege Monitor Screen

The **About Privilege Monitor** screen shows the current software version and build number.

### Database Contact Information



Database Contact Info

| | | | |
|---|---|---|---|
| **Database Connection Name** | gpOR816sun | **Application Name** | n/a |
| **Server Name/IP** | 192.168.3.21:1521 | **Database Location** | n/a |
| **Database Name** | oracle1 | | |
| **Region** | n/a | **Business Unit** | n/a |
| **Division** | n/a | **Usage** | n/a |
| **DBA1 Name** | n/a | **DBA2 Name** | n/a |
| **DBA1 Tel** | n/a | **DBA2 Tel** | n/a |
| **DBA1 Email** | n/a | **DBA2 Email** | n/a |

**Database Contact Info Screen**

You can invoke the **Database Contact Info** screen from the **Help -> Database Contact** menu. The database details given are:

- Database `Connection` Name
- Server Name/IP Address
- Database Name
- Region
- Division
- Application Name
- Database Location
- Business Unit
- Usage
- Contact Information for two DBAs.

# Configuring PM

There are three general parts of Privilege Monitor to configure:

- Schedules
- Receivers for Alert Email
- Guarded Items

## Setting Schedules

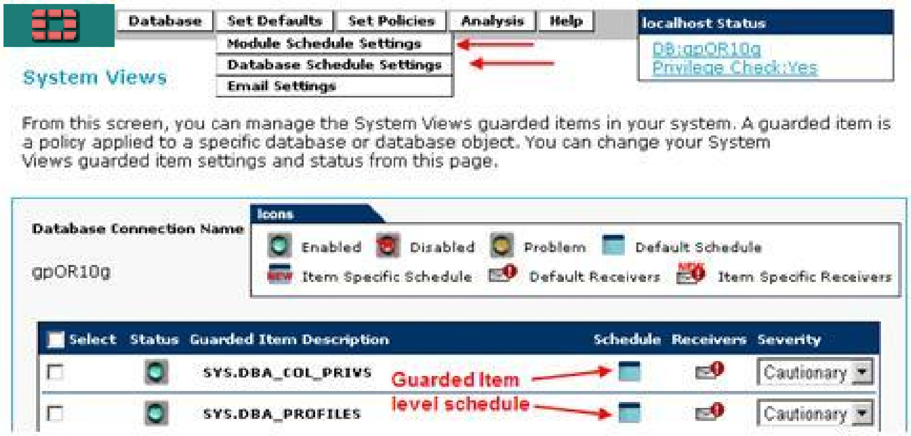
Scheduling is configured based upon two criteria:

- The type of time source to use for scheduling: timer- or calendar-based. For a timer-based schedule, you set a time interval for the monitoring. For a calendar-based schedule, you choose to have the monitoring run at a specific day and/or time. You can also combine the two.
- The scope of the schedule:
    - Module level: The entire PM module; a schedule that applies to all the databases, **System Views**, and UDRs
    - Database level: A particular database and its **System Views**, and UDRs within the module
    - Guarded Item[1] level: **System Views**, or UDRs within the database

If no other schedule is specified, the default-monitoring[2] schedule is every ten minutes. This applies to all databases and their contained **System Views**, and UDRs. If a Module level schedule is the only one set, it applies to all databases within that module. If a database level schedule is set, it will override any module level schedule for that particular database. If a Guarded Item-level schedule is set, it will override any module- or database-level schedule.

[1] *Guarded Items* are database objects (here System Views that you monitor directly) policies, or rules that you employ to monitor those objects. While sometimes used interchangeably, a *policy* is a best-business practice and a *rule* is the FortiDB-MA implementation of a policy.

[2] A *default* schedule is one used for monitoring in the absence of any other overriding schedule.



From this screen, you can manage the System Views guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your System Views guarded item settings and status from this page.

Database Connection Name: gpOR10g

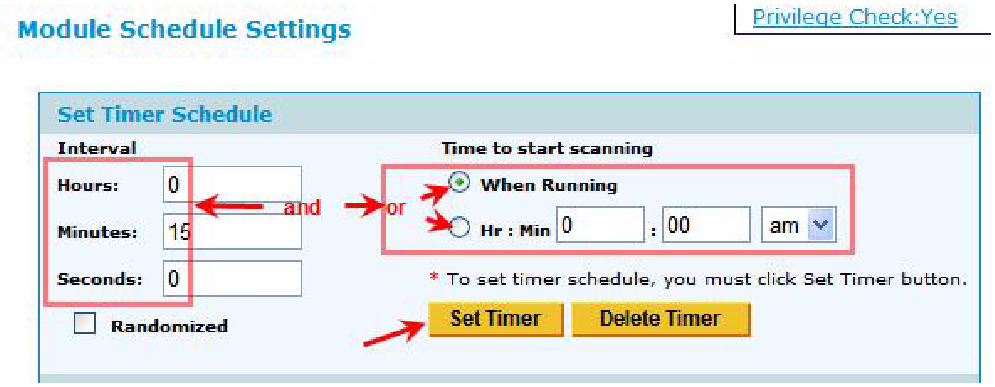
| Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| □ | ● | SYS.DBA_COL_PRIVS | ▨ | ✉ | Cautionary |
| □ | ● | SYS.DBA_PROFILES | ▨ | ✉ | Cautionary |

**Setting the Scope for a Schedule**

In order to configure a module- or database-level schedule, use the **Set Defaults -> Module Schedule Settings** menu or **Set Defaults -> Database Schedule Settings** menu.

In order to configure a Guarded Item-level schedule, click on the **Set Policies -> Schema Objects** menu. (Alternatively, the **Set Policies -> User-Defined Rule** menu), and then click on the Guarded Item-level **Schedule** icon in the row which contains the Guarded Item of interest.

## Setting a Timer-based Schedule



Interval

Hours: 0

Minutes: 15

Seconds: 0

□ Randomized

Time to start scanning

● When Running

○ Hr : Min 0 : 00 am

* To set timer schedule, you must click Set Timer button.

**Setting a Module-Wide, Timer-Based Schedule**

For a Timer-based Schedule:

1 Specify the monitoring **Interval** and the **Time to start scanning,** which will be either:

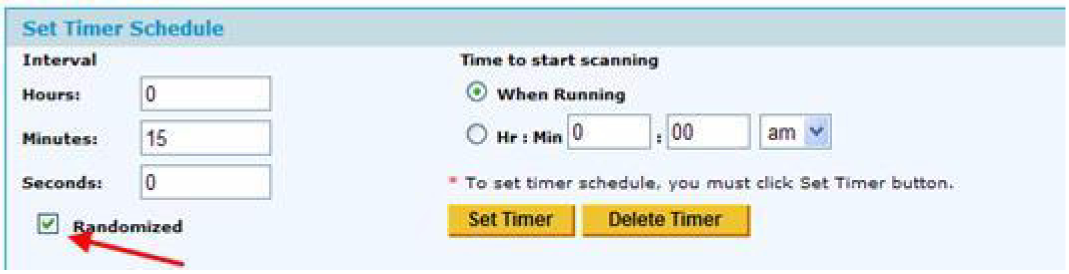
   a When Running: the chosen interval will be used whenever the database connection is **Open** and **Running**

   b Specific start time each day: the chosen interval will start being used at the time you specify. The database connection must be **Open** and **Running**

2 Click the **Set Timer** button in order to save the settings.

3 Click the **Delete Timer** button in order to delete either the **Interval** or **Time to start scanning** settings.

### Setting a Randomized Interval



Set Timer Schedule

Interval

Hours: 0

Minutes: 15

Seconds: 0

☑ Randomized

Time to start scanning

● When Running

○ Hr : Min 0 : 00 am

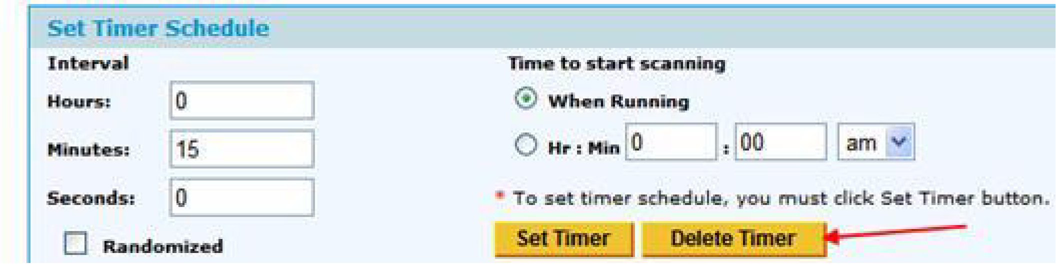
* To set timer schedule, you must click Set Timer button.

**Setting a Randomized Interval**

In order to make it difficult to predict your monitoring times, you can also set a monitor-reporting schedule that, while dependent on your chosen **Interval** value, will not run exactly that often.

If you check the **Randomized** checkbox, a random number is used to modify your specified interval in order to establish the time of the next monitoring. After each monitoring, the calculation is performed again--with another random number. This makes it extremely difficult to predict the time of your next monitoring, however, the average of all of the random-number-calculated intervals will, over time and after a sufficient number of monitoring evaluations, be equal to your specified interval.

## Deleting a Previously Set Timer Schedule



Set Timer Schedule

Interval

Hours: 0

Minutes: 15

Seconds: 0

□ Randomized

Time to start scanning

● When Running

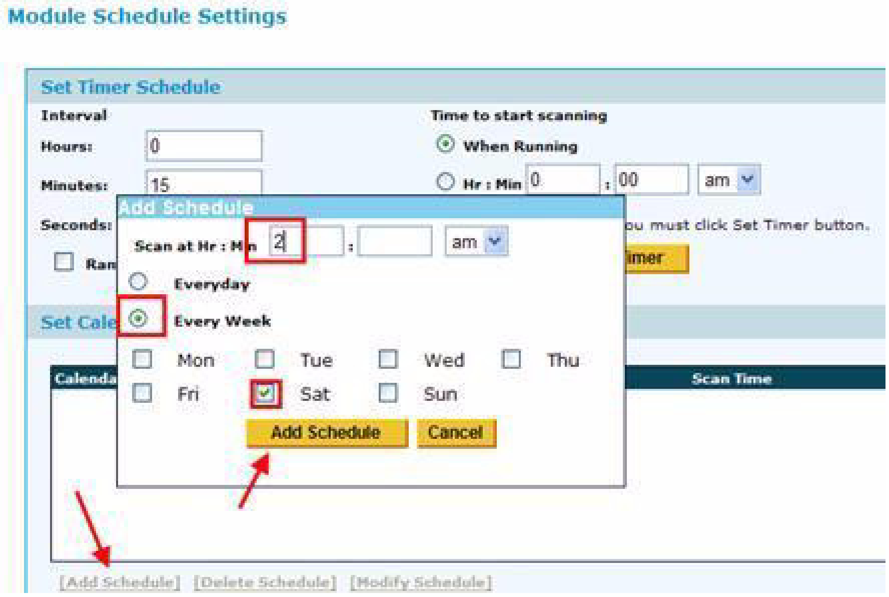
○ Hr : Min 0 : 00 am

* To set timer schedule, you must click Set Timer button.

**Deleting a Timer Schedule**

You can delete a previously set Timer schedule by clicking on the **Delete Timer** button.

### Setting a Calendar-based Schedule



Module Schedule Settings

Set Timer Schedule

Interval

Hours: 0

Minutes: 15

Seconds:

□ Ran

Time to start scanning

● When Running

○ Hr : Min 0 : 00 am

ou must click Set Timer button.

Set Cale

Add Schedule

Scan at Hr : Min 2 : am

○ Everyday

● Every Week

□ Mon □ Tue □ Wed □ Thu

□ Fri ☑ Sat □ Sun

**Set Module Schedule Setting Screen**

For a Calendar-based Schedule:

1 Click on the [Add Schedule] button at the bottom of the **Module Schedule Settings** screen.

2 Specify the monitoring days and/or times you want. In the example shown, we are setting up a schedule for the monitoring to occur each week on Saturday at 2 am.

3 Click on the **Add Schedule** button at the bottom of the **Add Schedule** popup screen in order to save the settings.

### Deleting a Calendar-based Schedule

In order to delete a calendar-based schedule, click on the **[Delete Schedule]** button on the **Module Schedule Settings** page.

### Setting a Combined Schedule

Your schedule can consist of both a timer- and a calendar-based schedule.

**Note:** To delete a combined schedule you will have to delete both the timer- and the calendar-based schedules.

## Configuring Receivers for Alert Emails

FortiDB MA allows you to configure an e-mail alert so that if a Guarded Item is enabled, disabled, or deleted, the FortiDB MA administrator will be notified. For more information, see the *FortiDB MA Administration Guide.*

# Setting Guarded Items

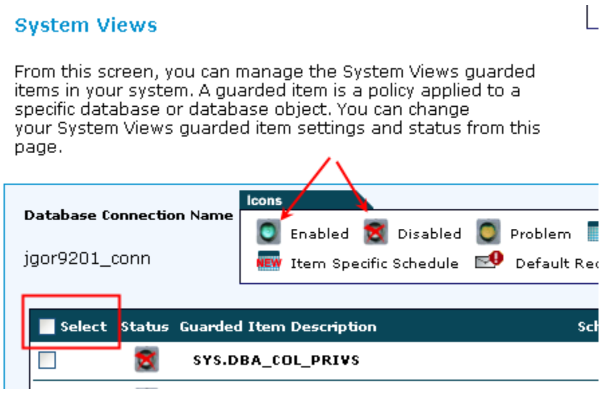
This section explains how to enable/disable Guarded Items, and change Guarded Item specific settings.

This section also explains two types of Guarded Items:

- System Views
- User-Defined Rules (UDR)

## Enabling Guarded Items

You can enable or disable your **Guarded Items** and their associated settings either together or on a **Guarded Item** specific basis.



System Views

From this screen, you can manage the System Views guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your System Views guarded item settings and status from this page.

Database Connection Name

jgor9201_conn

Icons

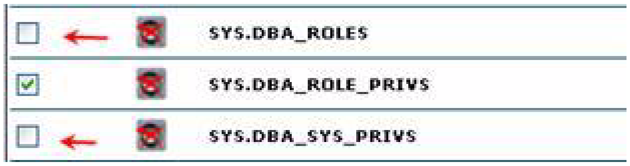
Enabled Disabled Problem

Item Specific Schedule Default Re

| □ Select | Status | Guarded Item Description | Sch |
|---|---|---|---|
| □ | | SYS.DBA_COL_PRIVS | |

**Configuring Guarded Items**

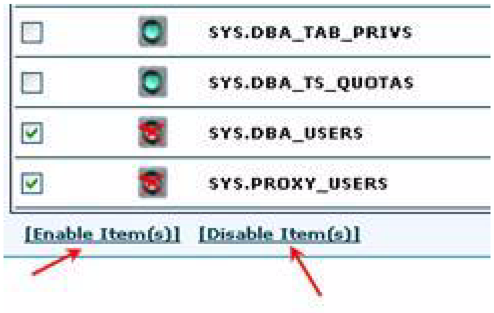
To choose all **Guarded Items** at once, check the **Select** checkbox in the header row. Moreover, if you uncheck the **Select** checkbox in the header row, all **Guarded Items** will be unselected.



| | | |
|---|---|---|
| □ | | SYS.DBA_ROLES |
| ☑ | | SYS.DBA_ROLE_PRIVS |
| □ | | SYS.DBA_SYS_PRIVS |

**Selecting Individual Guarded Items to Enable or Disable**

Alternatively, you can chose **Guarded Items** individually or make special groupings by checking the associated checkbox(es).

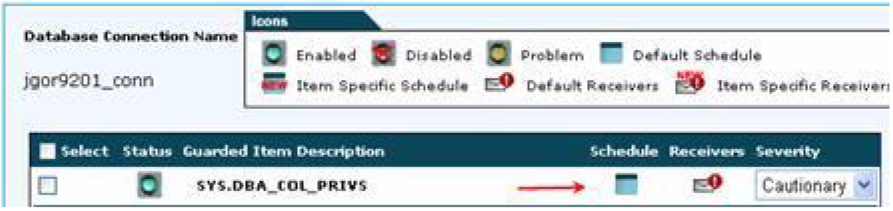


| | | |
|---|---|---|
| □ | ● | SYS.DBA_TAB_PRIVS |
| □ | ● | SYS.DBA_TS_QUOTAS |
| ☑ | ● | SYS.DBA_USERS |
| ☑ | ● | SYS.PROXY_USERS |

Enabling and Disabling rules

Clicking the **[Enable Item(s)]** or **[Disable Item(s)]** buttons at the button will then affect the **Guarded Items** you have chosen.

## Changing a Guarded Item-Specific Schedule



Database Connection Name

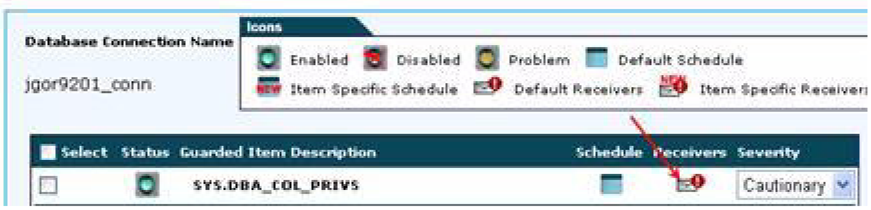
jgor9201_conn

| Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| □ | ● | SYS.DBA_COL_PRIVS | | | Cautionary |

**Setting Schedule**

The process for setting schedules at the module-, database-, and item- level is the same. Please see  Setting Schedules for a discussion of this topic.

## Changing Guarded Item-Specific Email Receivers



Database Connection Name

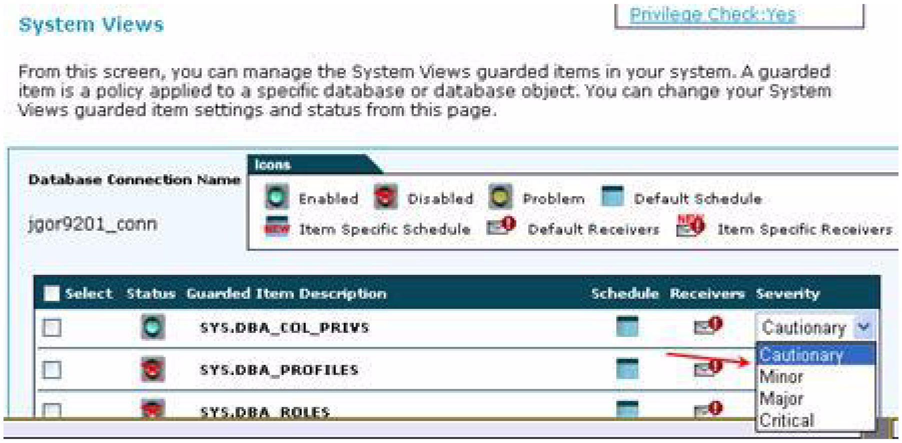
jgor9201_conn

| Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| □ | ● | SYS.DBA_COL_PRIVS | | | Cautionary |

**Setting Email Receivers**

Please see the *FortiDB MA Installation and Administration Guide* for a discussion of this topic.

## Changing a Guarded Item-Specific Severity Level



System Views

Privilege Check:Yes

From this screen, you can manage the System Views guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your System Views guarded item settings and status from this page.

Database Connection Name

jgor9201_conn

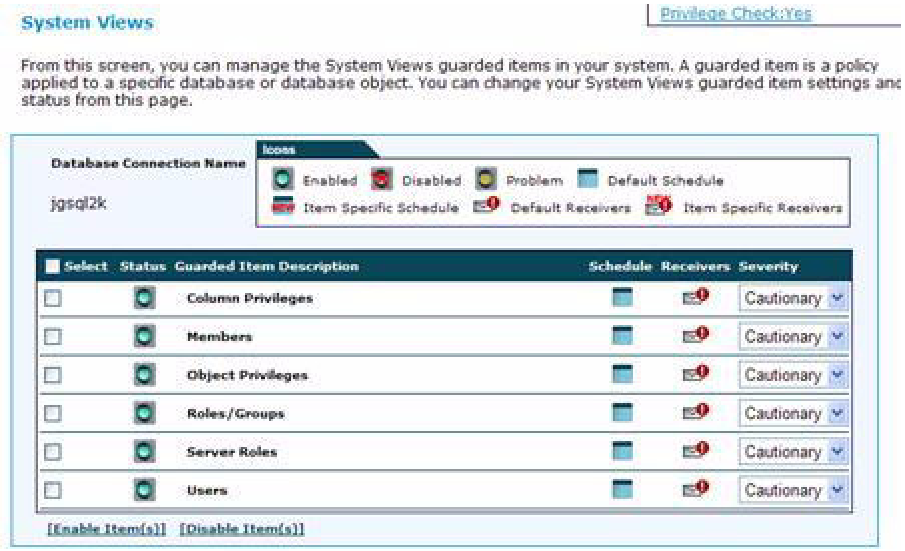
| ☐ Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| ☐ | ● | SYS.DBA_COL_PRIVS | | | Cautionary |
| ☐ | ● | SYS.DBA_PROFILES | | | |
| ☐ | ● | SYS.DBA_ROLES | | | |

**Changing a rule Severity Level**

In order to change a **Severity** level:

1. Click on the arrow to the right of the drop-down box in the **Severity** column for the particular **Guarded Item** of interest.
2. Choose a different **Severity** level.

# System Views



System Views

Privilege Check:Yes

From this screen, you can manage the System Views guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your System Views guarded item settings and status from this page.

Database Connection Name

jgsql2k

Icons

● Enabled ● Disabled ● Problem ▤ Default Schedule
▤ Item Specific Schedule ✉ Default Receivers ✉ Item Specific Receivers

| ☐ Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| ☐ | ● | Column Privileges | ▤ | ✉ | Cautionary ▾ |
| ☐ | ● | Members | ▤ | ✉ | Cautionary ▾ |
| ☐ | ● | Object Privileges | ▤ | ✉ | Cautionary ▾ |
| ☐ | ● | Roles/Groups | ▤ | ✉ | Cautionary ▾ |
| ☐ | ● | Server Roles | ▤ | ✉ | Cautionary ▾ |
| ☐ | ● | Users | ▤ | ✉ | Cautionary ▾ |

[Enable Item(s)] [Disable Item(s)]

**System Views (SQL Server example)**

**System Views** vary by RDBMS. Each database type will display a different list. For example, you can monitor **Column Privileges** as shown in the SQL Server screenshot above. The following tables describe RDBMS specific System Views.

**Note:** There are also RDBMS-specific Database Connection parameters**.**

# Oracle System Views

| System View Name | Contents | Description | Privileges Involved |
|---|---|---|---|
| SYS.DBA_COL_PRIVS | Column-level privilege granting | Gives you the ability to monitor column-level privilege changes. For example, user SCOTT can grant SELECT privileges on a column of a table to a user, without letting that user SELECT on other columns in the same table. | |
| SYS.DBA_PROFILES | Resources (I/O, etc.) assigned to users | Lists all resources and their limits. Changes to any profile setting could have wide-reaching effects. | |
| SYS.DBA_ROLES | Database roles | Contains information about all existing roles in the database. An Oracle role is a grouping of privileges. | |
| SYS.DBA_ROLE_PRIVS | Roles granted to users and other roles | Links users with their roles. It also contains information about which role has been assigned to other roles. Change of user's role means changes in user's access privileges. Role changes should be closely monitored in order to ensure data security. | |
| SYS.DBA_SYS_PRIVS | All granted system privileges | Contains all GRANTed system privileges to all users or roles. System privileges are powerful privileges and should be granted with great cautions. Monitoring system-privilege changes should be mandatory. | |
| SYS.DBA_TAB_PRIVS | All granted schema-object privileges | Lists all GRANTed privileges on schema objects. These include privileges on tables, views, sequences, procedures, functions and packages. | |
| SYS.DBA_TS_QUOTAS | Tablespace quotas assigned to users | Contains information about Tablespace quotas assigned to users. Oracle limits the amount of space that can be allocated for storage of a user's objects assigned quota. | |
| SYS.DBA_USERS | Database users | Contains information about users in the database. Although this view has no privilege information, it contains the users to whom privileges may be assigned or changed. | |

| | | | |
|---|---|---|---|
| **SYS.PROXY_USERS** | Users who can assume the identity of other users | Contains information about which user can assume the identity of another. Proxy users are typically employed in an environment with a middle tier, such as a firewall. | |

**Note:** SYS.DBA_TS_QUOTAS and SYS.PROXY_USERS always run with the snapshot (or **No Audit**) **Data Retrieval Method**, even if the database connection was defined with the **Data Retrieval Method** set to **Audit**. However, changing Tablespace quotas and changing proxy users are activities that can be monitored and can generate alerts. Both are monitored by SYS.DBA_USERS, which, in turn, monitors the use of the ALTER USER command. As a result, you will see two alerts generated for a single activity.

The two alerts come about in this manner. With the **Audit** method, when SYS.DBA_USERS is enabled, FortiDB MA issues an AUDIT USER command which causes CREATE/ALTER/DROP USER commands to be audited. In addition, these commands are used to not only manage database users but also Tablespace quotas and proxy users.

Consider, for example:

ALTER USER scott QUOTA UNLIMITED ON SYSTEM

This command generates an audit record whose action is ALTER USER because of AUDIT USER. This causes the PM Schema View, SYS.DBA_USERS, to generate the first of the two alerts. The ALTER USER command also causes a record to be added to the Oracle's dictionary view, SYS.DBA_TS_QUOTAS, in the target database. The PM Schema View, SYS.DBA_TS_QUOTAS, monitors the dictionary view (using the No Audit/snapshot method), detects this new record, and generates the second alert.

The CREATE USER and DROP USER commands may also add or remove records from the SYS.DBA_TS_QUOTAS and SYS.PROXY_USERS views. Like ALTER USER, those commands also allow you to specify Tablespace and proxy-user specifications.

# DB2 (NT/Unix) System Views

| System View Name | Contents | Description | Privileges Involved |
|---|---|---|---|
| SYSIBM.SYSCOLAUTH | Column privileges | | |
| SYSIBM.SYSDBAUTH | Database system privileges | | |
| SYSIBM.SYSINDEXAUTH | Index privileges | | This view contains the right to DROP the index. The creator of an index automatically has this CONTROL privilege. |
| SYSIBM.SYSPACKAGEAUTH | Package privileges | A package is a database object grouping related procedures, functions, associated cursors, and variables together. | CONTROL: Provides the ability to rebind, drop, execute, and extend these package privileges to others. Only SYSADM and DBADM authorities can grant CONTROL privilege.<br>BIND: Provides the privilege to rebind an existing package.<br>EXECUTE: Provides the privilege to execute a package. |
| SYSIBM.SYSSCHEMAAUTH | Schema privileges | Objects within a schema are: tables, views, indexes, packages, data types, functions, triggers, procedures, and aliases | CREATEIN: Provides the privilege to create objects within the schema.<br>ALTERIN: Provides the privilege to alter objects within the schema.<br>DROPIN: Provides the privilege to drop objects within the schema. |

| | | | |
|---|---|---|---|
| **SYSIBM.SYSTABAUTH** | Table privileges | | CONTROL: Provides the privilege to DROP the table or view and GRANT table or view privileges to somebody else.<br>ALTER: Provides the privilege to add columns, comments, primary key or unique constraint, in order to create triggers, and create or drop check constraints.<br>DELETE: Provides the privilege to delete rows.<br>INDEX: Provides the privilege to CREATE INDEX.<br>INSERT: Provides the privilege to INSERT rows.<br>REFERENCES: Provides the privilege to CREATE or DROP a foreign key.<br>SELECT: Provides the privilege to retrieve data.<br>UPDATE: Provides the privilege to change existing entries. |
| **SYSIBM.SYSTABSPACEAUTH** | Tablespace privileges | | A SYSADM or SYSCTRL authority can create Tablespace and grant USE privilege to others |

**Note:** DB2 does not require users or groups to be defined within the database; it depends on the underlying OS or other authentication mechanisms (e.g., DCE, LDAP, RACF) in order to perform user authentication.

# SQL Server System Views

| System View Name | Contents | Description | Privileges Involved |
|---|---|---|---|
| **Column Privileges** | `syscolumns` | | Column-level privileges |
| **Members** | `sysmembers` | | Role- and group-membership assignments |
| **Object Privileges** | `sysprotects` | | Column- and table-and other object-level privileges |
| **Roles[1]/Groups** | `sysobjects` | | All objects that are accessible<br>by the current user |
| **Server Roles** | `sp_helpservrolemember (a view)` | | Default server roles assigned to users. |
| **Users** | `sysusers` | | Lists valid database users and the groups to which they belong |

[1] When a database connection is established with the **Audit** radio button checked, alerts will not be generated when Application roles are created or dropped. (i.e. when the *sp_addapprole* and *sp_dropapprole* stored procedures are used.)

# Sybase Server System Views

| System View Name | Contents | Description | Privileges Involved |
|---|---|---|---|
| **Column Privileges** | `syscolumns` | | Column-level privileges |
| **Roles/Groups** | `sysobjects` | | All objects that are accessible<br>by the current user |
| **Members** | `sysmembers` | | Role- and group-membership assignments |
| **Object Privileges** | `sysprotects` | | Column- and table-and other object-level privileges |
| **Server Roles** | `sp_helpservrolemember (a view)` | | Default server roles assigned to users. |
| **Users** | `sysusers` | | Lists valid database users and the groups to which they belong |

**Note:** Sybase User Policies will generate alerts only for creating and deleting, not modifying, users.

# Changing System Views Settings

Privilege Monitor allows you to change System Views settings.

System Views are predefined views, created by the various RDBMS vendors, for viewing metadata objects and privileges without affecting the underlying system tables or catalogs. In general, **System Views** refer to user-related[1] metadata objects.

You can invoke the **System Views** screen from the **Set Policies -> System Views** menu. On the resulting screen, you may specify the following to start using **System Views**:

**System Views** become available when you create your database connection.

You cannot modify[2] **System Views** themselves; however, the following **System Views**-specific settings are available to you in order to implement company-specific monitoring requirements:

- Which Guarded Item(s) to enable or disable
- Guarded Item-specific Schedule
- Guarded Item-specific Receivers of violation notification via email
- Guarded Item-specific violation Severity

After configuring the necessary **System View** settings, **Privilege Checking** must be activated in order to detect potential violations and issue alerts. See Activating Privilege Checking and Checking Status for more information.

Further information that is provided in the **System Views** screen:

- Item Status (is it Enabled, and therefore to be monitored).
- Guarded Item Description (the name of the item)

[1] FortiDB-MA Privilege Monitor focuses on DDL statements involving users, while FortiDB-MA Metadata Monitor focuses on DDL statements involving objects..

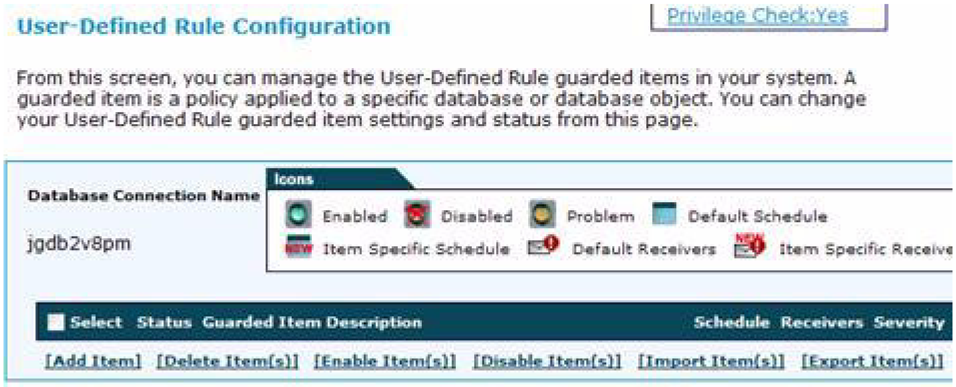
[2] FortiDB-MA offers you a User-Defined Rule (UDR) feature by which you can implement company specific security policies (See User-Defined Rules).

# User-Defined Rules

The **User-Defined Rules** (UDRs) feature allows you to write and manage rules specific to your organization. They can be written with SQL, or with a procedural language such as:

- PL/SQL (Oracle)
- Transact-SQL (SQL Server and Sybase)
- SQL Procedural Language (PL) (DB2)

You can access the **User-Defined Rule Configuration** screen with the **Set Policies -> User-Defined Rule** menu.



User-Defined Rule Configuration

From this screen, you can manage the User-Defined Rule guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your User-Defined Rule guarded item settings and status from this page.

Database Connection Name

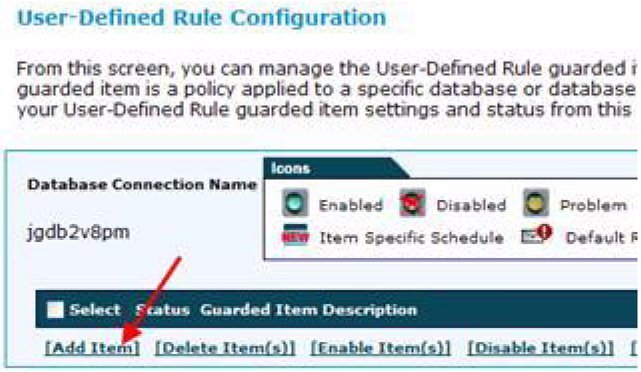
jgdb2v8pm

**User-Defined Rule Configuration Screen**

From the rule configuration page, you can perform managerial functions on UDRs such as:

- Adding
- Deleting
- Enabling
- Disabling
- Importing from a file
- Exporting to an XML file
- Setting severity
- Modifying (click on the Guarded Item Description to gain access)
- Setting monitor schedule
- Specifying email recipients

# Adding or Creating a UDR



User-Defined Rule Configuration

From this screen, you can manage the User-Defined Rule guarded i
guarded item is a policy applied to a specific database or database
your User-Defined Rule guarded item settings and status from this

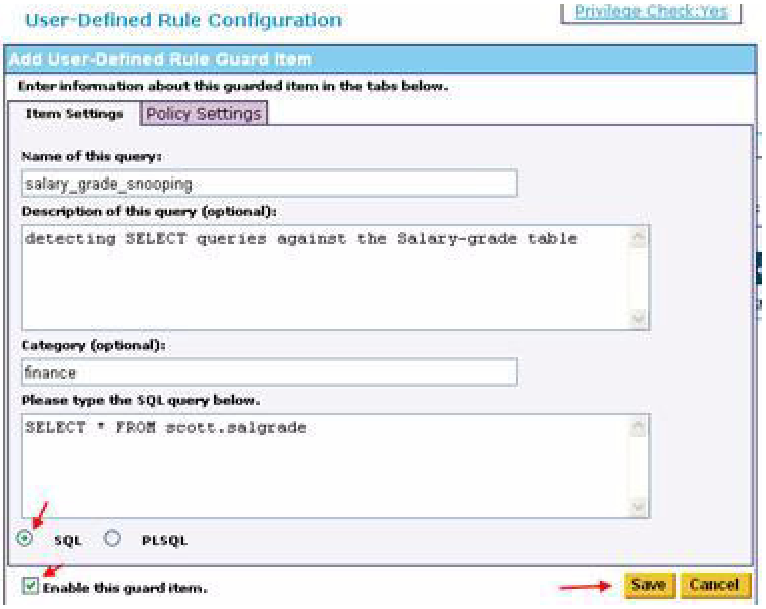
Database Connection Name

jgdb2v8pm

Icons
Enabled
Disabled
Problem
Item Specific Schedule
Default F
Select Status Guarded Item Description
[Add Item] [Delete Item(s)] [Enable Item(s)] [Disable Item(s)] [

**Adding a New UDR**

In order to create a UDR, select **Set Policies -> User-Defined Rule**, and then click on the **[Add Item]** button.



User-Defined Rule Configuration

Add User-Defined Rule Guard Item

Enter information about this guarded item in the tabs below.

Name of this query:
salary_grade_snooping

Description of this query (optional):
detecting SELECT queries against the Salary-grade table

Category (optional):
finance

Please type the SQL query below.

```
SELECT * FROM scott.salgrade
```

● SQL ○ PLSQL

☑ Enable this guard item.

**UDR Item Settings Tab Form (Oracle example)**

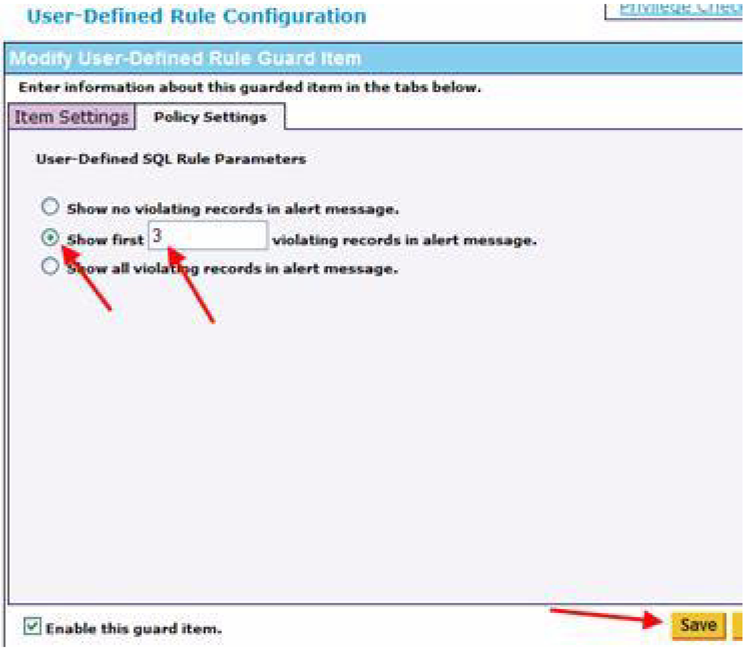
In order to configure your UDR, you must fill in the following on the **Item Settings** tab:

- The Name of this query
- The Please type the SQL query below field.

Optionally, you may also:

- Fill in the Category field in order to help you group your UDRs for reports
- Fill in the Description field in order to document your UDR
- Select the radio button for the language appropriate for your query (Oracle only):
  - SQL

- PLSQL


User-Defined Rule Configuration

Modify User-Defined Rule Guard Item

Enter information about this guarded item in the tabs below.

User-Defined SQL Rule Parameters

○ Show no violating records in alert message.

● Show first 3 violating records in alert message.

○ Show all violating records in alert message.

☑ Enable this guard item.

**UDR Policy Settings Tab Form**

After you have entered values in the **Item Settings** tab fields:

1 Check the **Policy Settings** tab to insure you are getting number of violating records per alert you want.

2 Click the **Save** button.

3 If you would like to enable the UDR immediately, check the **Enable this guard item** checkbox.

**Note:** After configuring the necessary UDR settings, **Privilege Checking** must be activated for alerts to be sent. Please refer to  Activating Privilege Checking and Checking Status for a discussion of this topic.

## Changing UDR Settings

You can invoke the **User-Defined Rule** screen from the **Set Policies -> User-Defined Rule** menu. From the resulting screen, you can specify:

- Which Guarded Item(s) to enable or disable
- Guarded Item-specific Schedule
- Guarded Item-specific Receivers of violation notification via email
- Guarded Item-specific violation Severity

After configuring the necessary UDR settings, **Privilege Checking** must be activated in order to detect potential violations and issue alerts. See  Activating Privilege Checking and Checking Statusfor more information.

Further information that is provided in the System View screen:

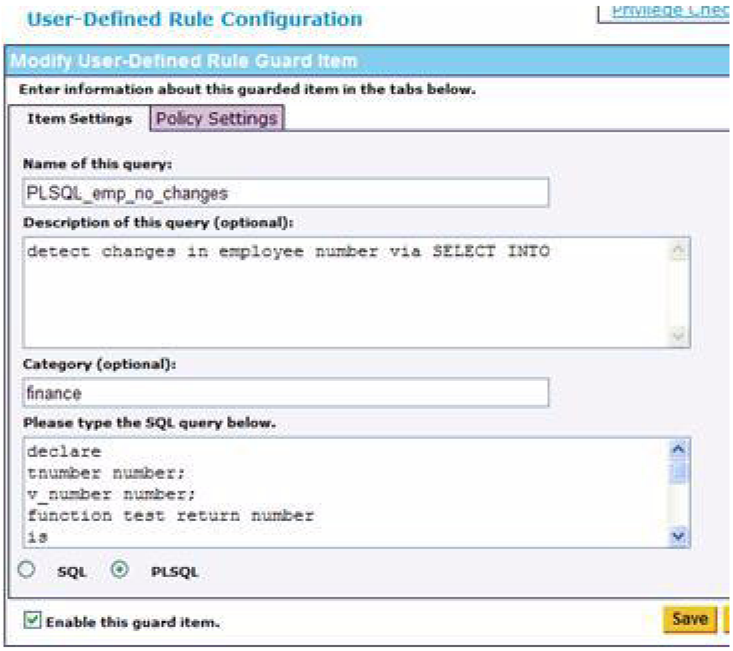
- Item Status (is it Enabled, and therefore to be monitored).
- Guarded Item Description (the name of the item)

For details on changing **UDR** (Guarded Item) Settings, please refer to Changing UDR Settings.

# User-Defined Rules by RDBMS

This section explains User-Defined Rules by Oracle PL/SQL, Transact SQL for MS SQL Server, and SQL Procedural Language for DB2.

## PL/SQL User-Defined Rules (Oracle)


User-Defined Rule Configuration
Privilege Chec
Modify User-Defined Rule Guard Item
Item Settings
Policy Settings
Save

Enter information about this guarded item in the tabs below.

Name of this query: PLSQL_emp_no_changes

Description of this query (optional): detect changes in employee number via SELECT INTO

Category (optional): finance

Please type the SQL query below.

```
declare
tnumber number;
v_number number;
function test return number
is
```

○ SQL ● PLSQL

☑ Enable this guard item.

Adding a PL/SQL Rule

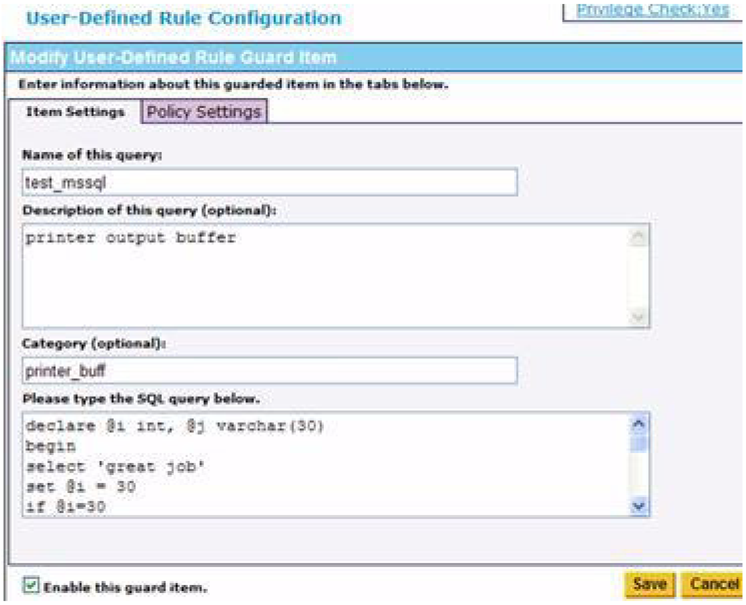
### Example:

```
declare
tnumber number;
v_number number;
function test return number
is
begin
   select empno  into tnumber from scott.emp where
empno=7900;
   return tnumber;
end;
begin
```

```
      v_number := test;
      update scott.emp set sal=8000 where empno= v_number;
   end;
```

**Note:** Oracle users must specify if they wish to use SQL or PL/SQL statements by selecting the appropriate button prior to saving and enabling this guarded policy.

## Transact SQL User-Defined Rules (SQL Server)


User-Defined Rule Configuration
Privilege Check:Yes
Modify User-Defined Rule Guard Item
Item Settings
Policy Settings
Save
Cancel

Enter information about this guarded item in the tabs below.

Name of this query: test_mssql

Description of this query (optional): printer output buffer

Category (optional): printer_buff

Please type the SQL query below.

```
declare @i int, @j varchar(30)
begin
select 'great job'
set @i = 30
if @i=30
```

☑ Enable this guard item.

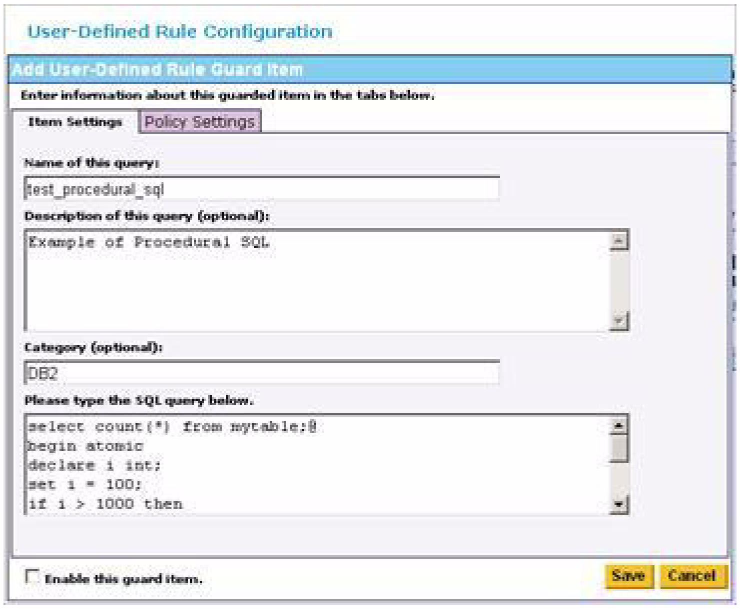
**Adding a Transact SQL Rule**

### Example:

```
declare @i int, @j varchar(30)
begin
   select 'great job'
   set @i = 30
   if @i=30
         begin
            set @i = @i + 1
            set @j = 'equal to 30'
            print ' equal to 30 '
            select @j
         end
         if @i=31 select 'greater than 30'
         while @i<35
         begin
            set @i=@i+1
            select @i
         end
```

```
end
```

## SQL Procedural Language User-Defined Rules (DB2)


User-Defined Rule Configuration
Add User-Defined Rule Guard Item
Item Settings
Policy Settings
Save
Cancel

Enter information about this guarded item in the tabs below.

Name of this query: test_procedural_sql

Description of this query (optional): Example of Procedural SQL

Category (optional): DB2

Please type the SQL query below.

```
select count(*) from mytable;@
begin atomic
declare i int;
set i = 100;
if i > 1000 then
```

□ Enable this guard item.

**Adding a Procedural SQL Rule**

**Note:** FixPak 4 for DB2 UDB 7.2 AIX client must be installed in order to support this feature.

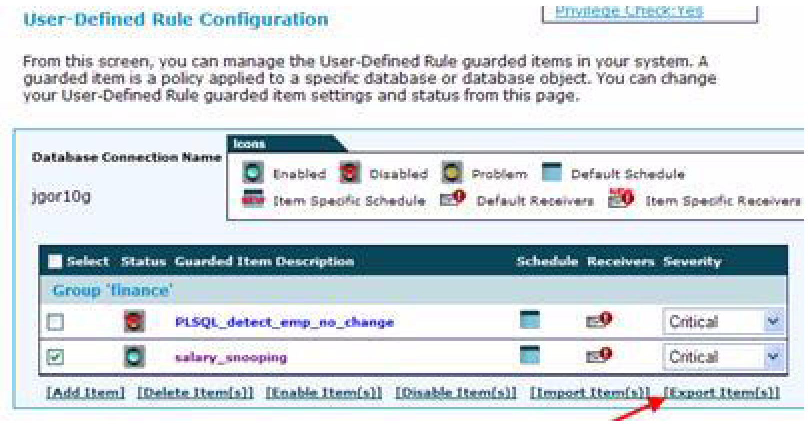
### Example

```
select count(*) from mytable;@
begin atomic
   declare i int;
   set i = 100;
   if i > 1000 then
         signal sqlstate 'IPERR'  set message_text = '
Something is \[1]
         wrong';
   end if;
   insert into mytable values(10);
end@
```

select count(*) from mytable;@

[1] Line continuation symbol that is not actually keyed.

# Exporting User-Defined Rules



User-Defined Rule Configuration

From this screen, you can manage the User-Defined Rule guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your User-Defined Rule guarded item settings and status from this page.

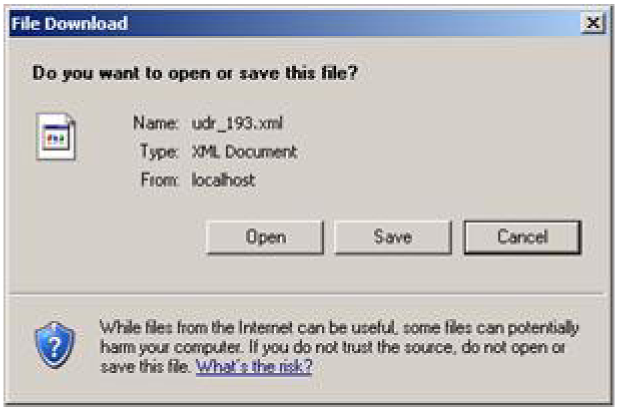
Database Connection Name: jgor10g

| Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| Group 'finance' | | | | | |
| □ | ● | PLSQL_detect_emp_no_change | | | Critical |
| ☑ | ● | salary_snooping | | | Critical |

[Add Item] [Delete Item(s)] [Enable Item(s)] [Disable Item(s)] [Import Item(s)] [Export Item(s)]

**Exporting a UDR**

PM allows you to export your UDRs to an XML file, permitting you to transfer UDRs from one FortiDB MA installation to another. From the **User-Defined Rule Configuration** screen, select one or more rules to Export and click the **[Export Item(s)]** button.



File Download

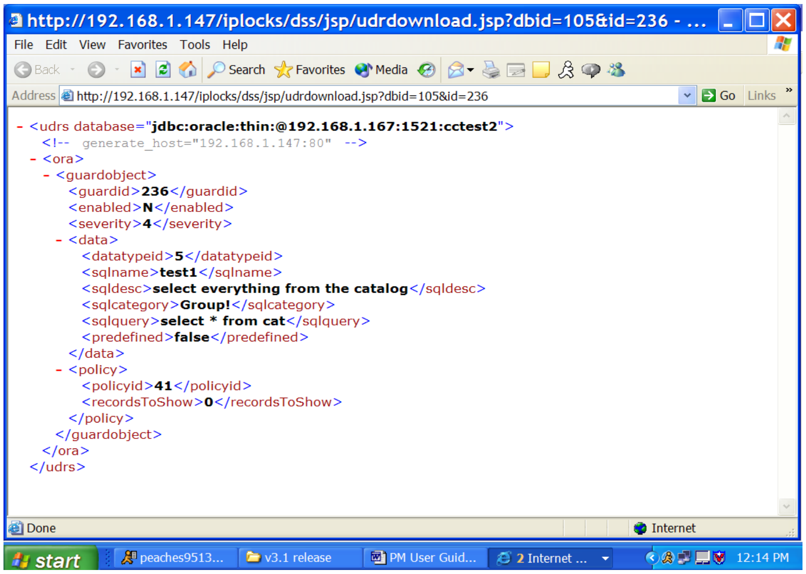
Do you want to open or save this file?

Name: udr_193.xml
Type: XML Document
From: localhost

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

**Exporting Dialog Box**

You will then be asked if you would like to **Open** or **Save** the XML file.



http://192.168.1.147/iplocks/dss/jsp/udrdownload.jsp?dbid=105&id=236 - ...

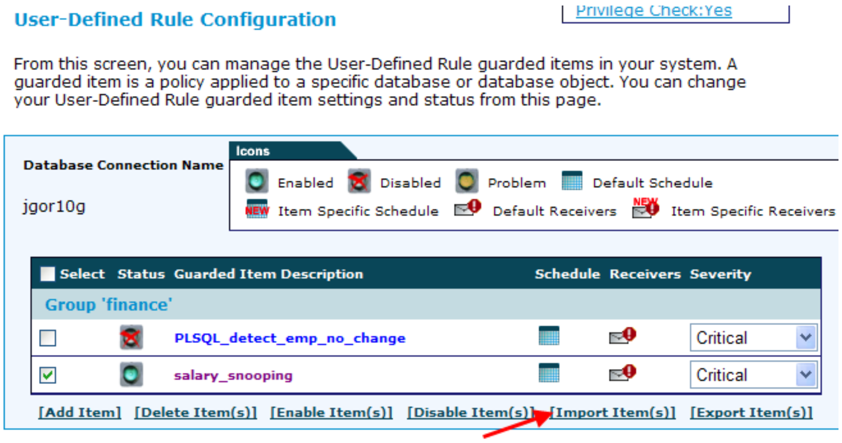
Address: http://192.168.1.147/iplocks/dss/jsp/udrdownload.jsp?dbid=105&id=236

```
- <udrs database="jdbc:oracle:thin:@192.168.1.167:1521:cctest2">
    <!--  generate_host="192.168.1.147:80"  -->
  - <ora>
    - <guardobject>
        <guardid>236</guardid>
        <enabled>N</enabled>
        <severity>4</severity>
      - <data>
          <datatypeid>5</datatypeid>
          <sqlname>test1</sqlname>
          <sqldesc>select everything from the catalog</sqldesc>
          <sqlcategory>Group!</sqlcategory>
          <sqlquery>select * from cat</sqlquery>
          <predefined>false</predefined>
        </data>
      - <policy>
          <policyid>41</policyid>
          <recordsToShow>0</recordsToShow>
        </policy>
      </guardobject>
    </ora>
  </udrs>
```

**XML File Containing a UDR (seen after clicking Open)**

If you elect to save, a standard Save As dialog box will appear

# Importing User-Defined Rules



User-Defined Rule Configuration

Privilege Check:Yes

From this screen, you can manage the User-Defined Rule guarded items in your system. A guarded item is a policy applied to a specific database or database object. You can change your User-Defined Rule guarded item settings and status from this page.

Database Connection Name

jgor10g

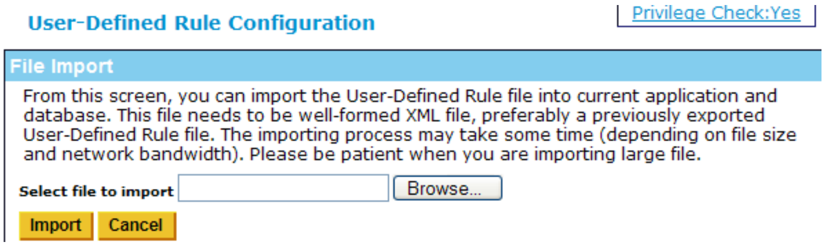
| Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| Group 'finance' | | | | | |
| □ | Disabled | PLSQL_detect_emp_no_change | Default Schedule | Default Receivers | Critical |
| ☑ | Enabled | salary_snooping | Default Schedule | Default Receivers | Critical |

[Add Item] [Delete Item(s)] [Enable Item(s)] [Disable Item(s)] [Import Item(s)] [Export Item(s)]

**Import Item(s)] Button for Importing a UDR**

You can import UDR definitions from an XML file to utilize UDRs developed on another FortiDB MA system.

From the **User-Defined Rule Configuration** screen, click the **[Import Item(s)]** button.



User-Defined Rule Configuration

File Import

From this screen, you can import the User-Defined Rule file into current application and database. This file needs to be well-formed XML file, preferably a previously exported User-Defined Rule file. The importing process may take some time (depending on file size and network bandwidth). Please be patient when you are importing large file.

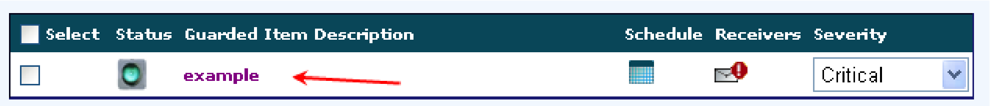
Select file to import

**Importing a UDR**

You will then be prompted to enter (or **Browse** to find) the name of the XML file, which contains your rule definition(s).

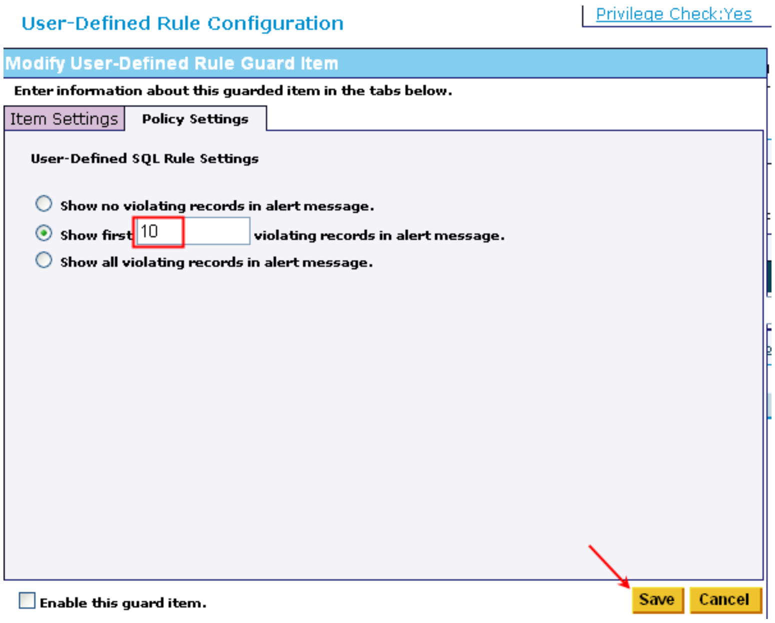
## Changing the Number of Violations Shown

This feature is available for User-Defined Rules, but not System Views.



| □ Select | Status | Guarded Item Description | Schedule | Receivers | Severity |
|---|---|---|---|---|---|
| □ | ● | example | ▦ | ✉ | Critical |

**Guarded Item Description**



User-Defined Rule Configuration

Modify User-Defined Rule Guard Item

Enter information about this guarded item in the tabs below.

User-Defined SQL Rule Settings

○ Show no violating records in alert message.

● Show first 10 violating records in alert message.

○ Show all violating records in alert message.

□ Enable this guard item.

Rule Policy Settings Tab

In order to change the number of violations shown per alert message:

1. Click on the **Guarded Item Description**
2. Go to the **Policy Settings** tab.
3. Modify the violating records per message setting.
4. Click the **Save** button.

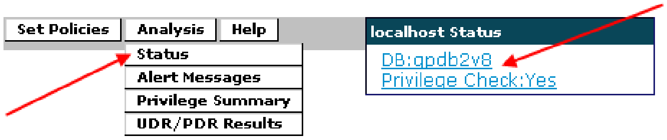
# Activating Privilege Checking and Checking Status

In order to generate alerts for **System Views**, UDRs, **Privilege Checking** must be activated. Furthermore, your database must be **Open and Running**, not just **Open**.

The **Status** screen:

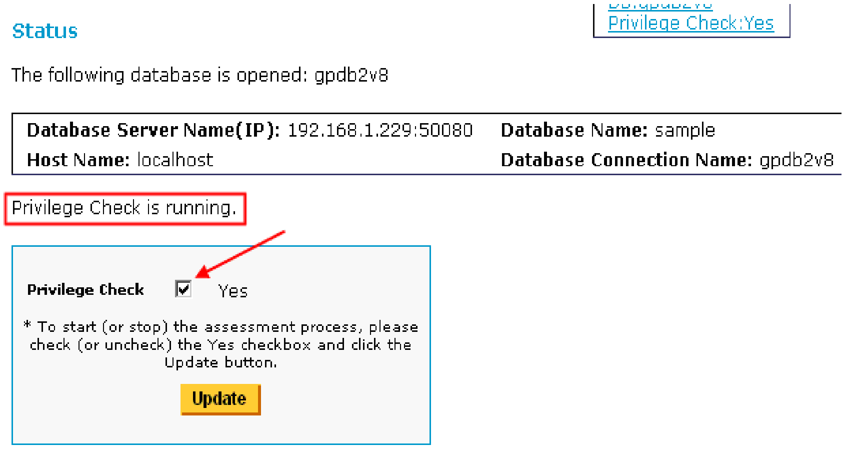
- Allows activation of Privilege Checking
- Displays information about the currently
- Open, though not necessarily Open and Running, database

## Activating Privilege Checking



**Navigating to the Status Screen**

In order to activate **Privilege Checking** for a database, go to the **Status** screen, select the **Analysis -> Status menu,** or click on the **Privilege Check** button on the upper right portion of the screen.



Status

The following database is opened: gpdb2v8

**Database Server Name(IP):** 192.168.1.229:50080 **Database Name:** sample
**Host Name:** localhost **Database Connection Name:** gpdb2v8

Privilege Check is running.

**Privilege Check** ☑ Yes

* To start (or stop) the assessment process, please check (or uncheck) the Yes checkbox and click the Update button.

**Determining and Setting Privilege-Checking Status**

To activate **Privilege Checking** from the **Status** screen, check the **Privilege Check** checkbox, and then click **Update**.

# Checking Status

The **Status** screen only displays information about databases that are **Open,** or **Open and Run**ning, but not those that are closed. The selected database is listed on the right end of the menu.

You can invoke the **Status** screen from the **Analysis -> Status** menu.

The **Status** screen gives information on the:

- Database Server Name or IP address
- Database Name or IP address
- Host Name
- Database Connection Name
- Status of Privilege Checking

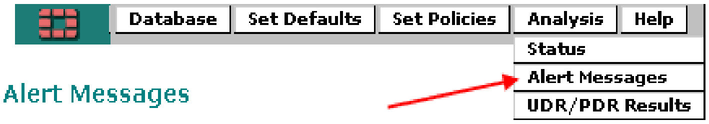
# Analyzing Alerts

Alerts warn you of potential security weaknesses in your database. Privilege Monitor offers three ways of detecting weakness:

- Alert Messages
- Privilege Summary
- UDR Results

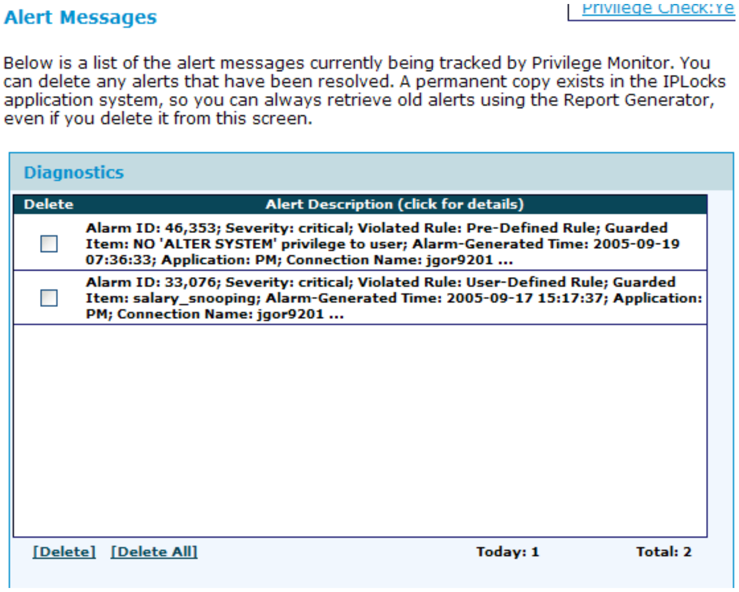
## Alert Messages

The specific alerts you receive depend upon which **System Views**, and UDRs you have enabled. (Alternately, you can also get alert information via email. See Configuring Receivers for Alert Emails.)



**Accessing Alert Messages**

To view **Alert Messages**, click on the **Analysis** -> **Alert Messages** menu.



Privilege Check:Ye

Alert Messages

Below is a list of the alert messages currently being tracked by Privilege Monitor. You can delete any alerts that have been resolved. A permanent copy exists in the IPLocks application system, so you can always retrieve old alerts using the Report Generator, even if you delete it from this screen.

Diagnostics

| Delete | Alert Description (click for details) |
|---|---|
| □ | Alarm ID: 46,353; Severity: critical; Violated Rule: Pre-Defined Rule; Guarded Item: NO 'ALTER SYSTEM' privilege to user; Alarm-Generated Time: 2005-09-19 07:36:33; Application: PM; Connection Name: jgor9201 ... |
| □ | Alarm ID: 33,076; Severity: critical; Violated Rule: User-Defined Rule; Guarded Item: salary_snooping; Alarm-Generated Time: 2005-09-17 15:17:37; Application: PM; Connection Name: jgor9201 ... |

[Delete] [Delete All] Today: 1 Total: 2

**Alert Messages Screen**

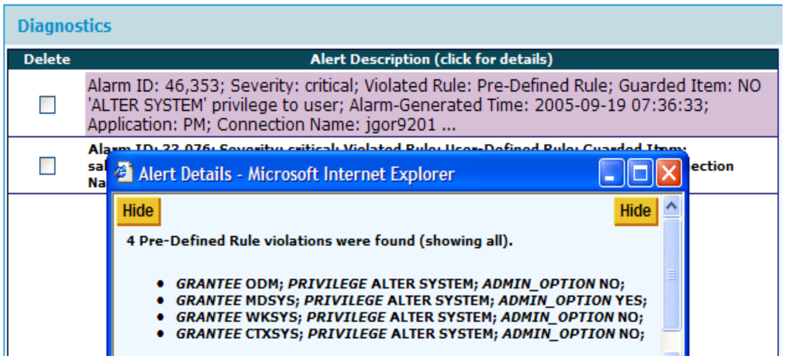
From the **Alert Message** screen, you can delete any alerts. A permanent copy exists in the FortiDB MA internal database, so you can always retrieve old alerts using the **Reporting** utility[1], even if you have deleted them from this screen.

[1] Please see the FortiDB-MA Utility User Guide for a discussion of these topics.

If you want to delete only certain alerts, first check the **Delete** checkbox in the row of interest and then click on the **Delete** button. In order to delete all alerts at once, click on the **Delete All** button.

The content of the alert messages includes:

| *Alert Field* | *Description* |
|---|---|
| **Alarm ID** | Unique number assigned by FortiDB MA |
| **Severity** | User defined severity level (cautionary, minor, major, or critical) |
| **Violated Rule** | Type of rule violated (System View, or UDR) |
| **Guarded item** | Guarded Item Description |
| **Alarm-Generated Time** | Day and time alert was generated |
| **Application** | FortiDB MA module involved (here PM) |
| **Connection Name** | User-assigned name of database connection |



Diagnostics

| Delete | Alert Description (click for details) |
|---|---|
| □ | Alarm ID: 46,353; Severity: critical; Violated Rule: Pre-Defined Rule; Guarded Item: NO 'ALTER SYSTEM' privilege to user; Alarm-Generated Time: 2005-09-19 07:36:33; Application: PM; Connection Name: jgor9201 ... |
| □ | Alarm ID: 33,076; Severity: critical; Violated Rule: User-Defined Rule; Guarded Item: sal ection Na |

Alert Details - Microsoft Internet Explorer

4 Pre-Defined Rule violations were found (showing all).

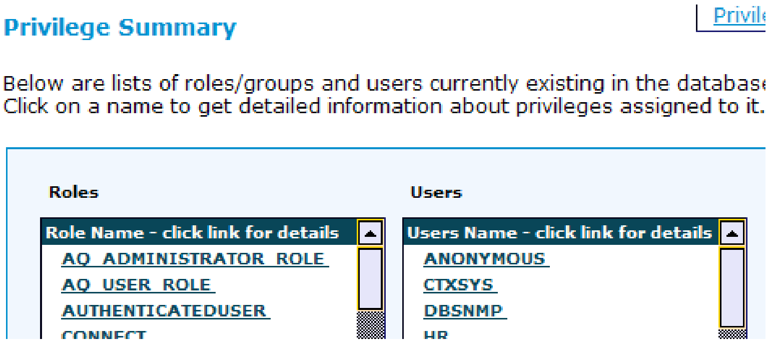
- *GRANTEE* ODM; *PRIVILEGE* ALTER SYSTEM; *ADMIN_OPTION* NO;
- *GRANTEE* MDSYS; *PRIVILEGE* ALTER SYSTEM; *ADMIN_OPTION* YES;
- *GRANTEE* WKSYS; *PRIVILEGE* ALTER SYSTEM; *ADMIN_OPTION* NO;
- *GRANTEE* CTXSYS; *PRIVILEGE* ALTER SYSTEM; *ADMIN_OPTION* NO;

**Alert Message Detail**

By clicking on the **Alert Description**, a dialog box with more detailed information about the alert of the Guarded Item will open.

**Note:** When viewing a large numbers of alerts, it may take several minutes for the system to process all of the messages in order to produce the **Alert Messages** page.

# Privilege Summary



Below are lists of roles/groups and users currently existing in the databas
Click on a name to get detailed information about privileges assigned to it.

| Roles | Users |
|---|---|
| Role Name - click link for details | Users Name - click link for details |
| AQ_ADMINISTRATOR_ROLE | ANONYMOUS |
| AQ_USER_ROLE | CTXSYS |
| AUTHENTICATEDUSER | DBSNMP |
| CONNECT | HR |

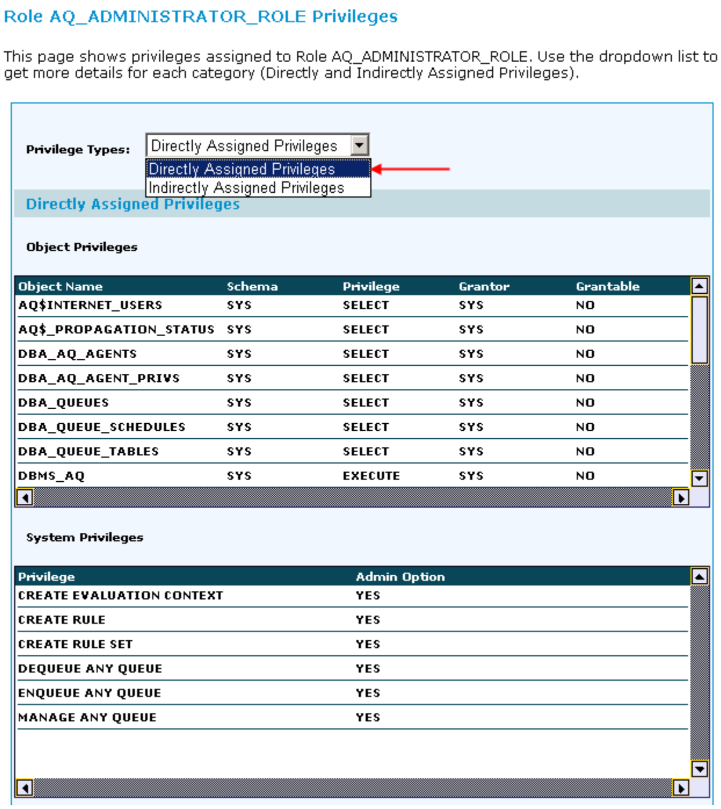
**Privilege Summary Screen (Oracle example)**

A **Privilege Summary** enables you to see, in one place, the **Users** and **Roles**/**Groups** that exist in a particular database, with the privileges assigned to each.

You can invoke the **Privilege Summary** screen from the **Analysis -> Privilege Summary** menu.

There are slight differences by RDBMS type:

- Users is a distinction used for all RDBMS types.
- Roles are used for all RDBMS types except DB2.
- Groups are used in just DB2.



Role AQ_ADMINISTRATOR_ROLE Privileges

This page shows privileges assigned to Role AQ_ADMINISTRATOR_ROLE. Use the dropdown list to get more details for each category (Directly and Indirectly Assigned Privileges).

Privilege Types: Directly Assigned Privileges

Directly Assigned Privileges

Object Privileges

| Object Name | Schema | Privilege | Grantor | Grantable |
|---|---|---|---|---|
| AQ$INTERNET_USERS | SYS | SELECT | SYS | NO |
| AQ$_PROPAGATION_STATUS | SYS | SELECT | SYS | NO |
| DBA_AQ_AGENTS | SYS | SELECT | SYS | NO |
| DBA_AQ_AGENT_PRIVS | SYS | SELECT | SYS | NO |
| DBA_QUEUES | SYS | SELECT | SYS | NO |
| DBA_QUEUE_SCHEDULES | SYS | SELECT | SYS | NO |
| DBA_QUEUE_TABLES | SYS | SELECT | SYS | NO |
| DBMS_AQ | SYS | EXECUTE | SYS | NO |

System Privileges

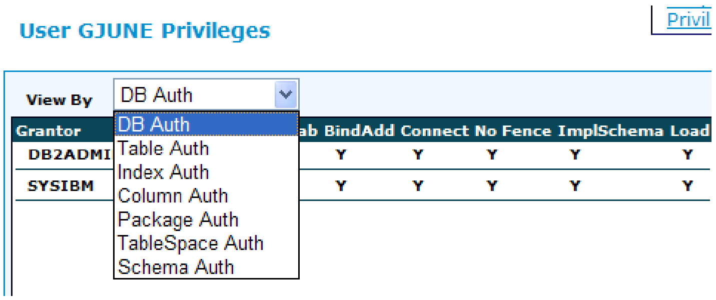
| Privilege | Admin Option |
|---|---|
| CREATE EVALUATION CONTEXT | YES |
| CREATE RULE | YES |
| CREATE RULE SET | YES |
| DEQUEUE ANY QUEUE | YES |
| ENQUEUE ANY QUEUE | YES |
| MANAGE ANY QUEUE | YES |

**Assigned Privileges Screen (Oracle example)**

If you click on an individual user, role, or group on any **Privilege Summary** screen, you can get a list of the specific **Object** and **System Privileges** assigned—both directly and indirectly[1]. For example, when clicking on the `AQ_ADMINISTRATOR_ROLE` while connected to an Oracle database, you would see the screen above, populated by having used **Directly Assigned Privileges** setting.

For all RDBMS types except DB2, you can filter privileges by either:

- Directly Assigned
- Indirectly Assigned



User GJUNE Privileges

View By: DB Auth

| Grantor | ab | BindAdd | Connect | No Fence | ImplSchema | Load |
|---|---|---|---|---|---|---|
| DB2ADMI | | Y | Y | Y | Y | Y |
| SYSIBM | | Y | Y | Y | Y | Y |

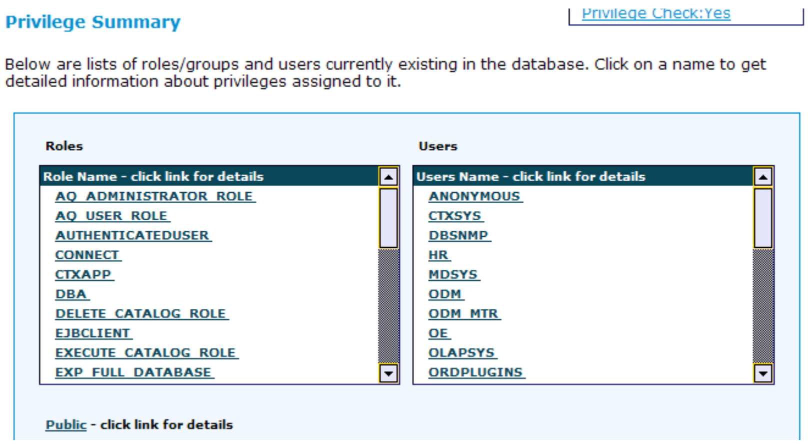
**DB2 Authorization Types**

For DB2 you can filter by these authorization types:

[1] Indirectly assigned privileges are those implicitly given by being a member of a role or group.

- DB
- Table
- Index
- Column
- Package
- Tablespace
- Schema

## Oracle Privilege Summary



Privilege Summary

Privilege Check:Yes

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Roles

| Role Name - click link for details |
|---|
| AQ_ADMINISTRATOR_ROLE |
| AQ_USER_ROLE |
| AUTHENTICATEDUSER |
| CONNECT |
| CTXAPP |
| DBA |
| DELETE_CATALOG_ROLE |
| EJBCLIENT |
| EXECUTE_CATALOG_ROLE |
| EXP_FULL_DATABASE |

Users

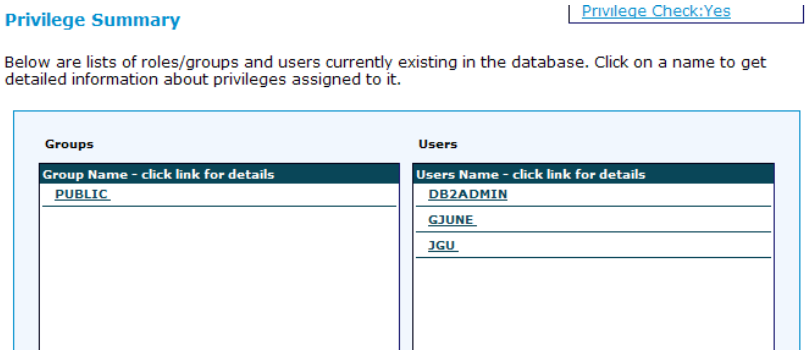
| Users Name - click link for details |
|---|
| ANONYMOUS |
| CTXSYS |
| DBSNMP |
| HR |
| MDSYS |
| ODM |
| ODM_MTR |
| OE |
| OLAPSYS |
| ORDPLUGINS |

Public - click link for details

**Privilege Summary Screen (Oracle)**

The Oracle **Privilege Summary** screen shows the **Roles** and **Users** that have been granted privileges within the currently connected database.

## DB2 Privilege Summary



Privilege Summary

Privilege Check:Yes

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Groups

| Group Name - click link for details |
|---|
| PUBLIC |

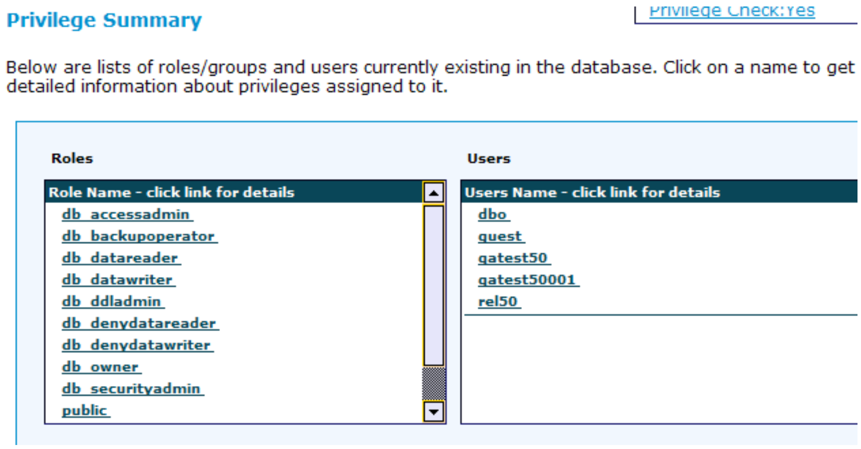
Users

| Users Name - click link for details |
|---|
| DB2ADMIN |
| GJUNE |
| JGU |

**Privilege Summary Screen (DB2)**

The DB2 **Privilege Summary** screen shows the **Groups** and **Users** that have been granted privileges within the currently connected database.

# *SQL Server Privilege Summary*



Privilege Summary

Privilege Check:Yes

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Roles

| Role Name - click link for details |
|---|
| db_accessadmin |
| db_backupoperator |
| db_datareader |
| db_datawriter |
| db_ddladmin |
| db_denydatareader |
| db_denydatawriter |
| db_owner |
| db_securityadmin |
| public |

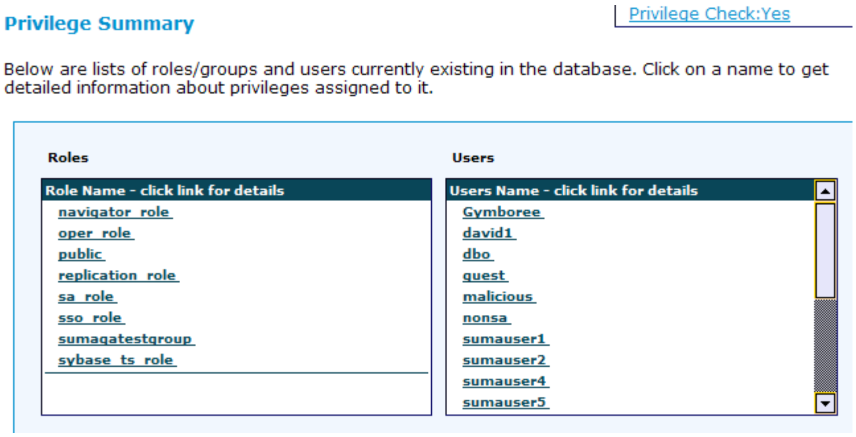
Users

| Users Name - click link for details |
|---|
| dbo |
| guest |
| qatest50 |
| qatest50001 |
| rel50 |

**Privilege Summary Screen (SQL Server)**

The SQL Server **Privilege Summary** screen shows the **Roles** and **Users** that have been granted privileges within the currently connected database.

# Sybase Privilege Summary



Privilege Summary

Privilege Check:Yes

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Roles

| Role Name - click link for details |
|---|
| navigator_role |
| oper_role |
| public |
| replication_role |
| sa_role |
| sso_role |
| sumaqatestgroup |
| sybase_ts_role |

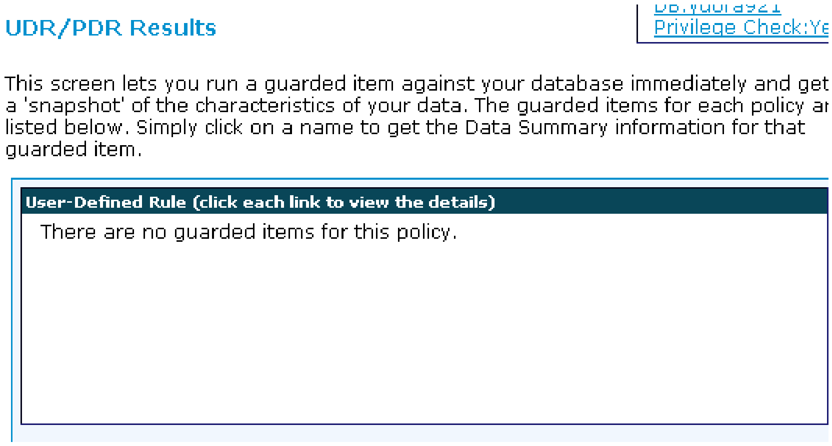
Users

| Users Name - click link for details |
|---|
| Gymboree |
| david1 |
| dbo |
| guest |
| malicious |
| nonsa |
| sumauser1 |
| sumauser2 |
| sumauser4 |
| sumauser5 |

**Privilege Summary Screen (Sybase)**

The Sybase **Privilege Summary** screen shows the **Roles** and **Users** that have been granted privileges within the currently connected database.

# UDR Results



UDR/PDR Results

Privilege Check:Ye

This screen lets you run a guarded item against your database immediately and get a 'snapshot' of the characteristics of your data. The guarded items for each policy ar listed below. Simply click on a name to get the Data Summary information for that guarded item.

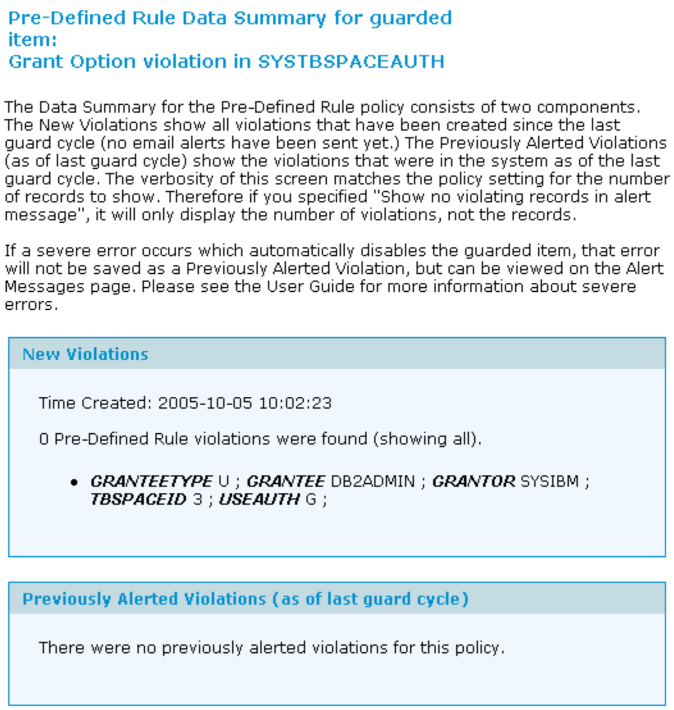
**User-Defined Rule (click each link to view the details)**

There are no guarded items for this policy.

**UDR Results Screen (Oracle example)**

The purpose of this feature is to test individual **User-Defined** and **Pre-Defined Rules**.

You can invoke the **UDR/PDR Results** screen from the **Analysis -> UDR/PDR Results** menu.



Pre-Defined Rule Data Summary for guarded item:
Grant Option violation in SYSTBSPACEAUTH

The Data Summary for the Pre-Defined Rule policy consists of two components. The New Violations show all violations that have been created since the last guard cycle (no email alerts have been sent yet.) The Previously Alerted Violations (as of last guard cycle) show the violations that were in the system as of the last guard cycle. The verbosity of this screen matches the policy setting for the number of records to show. Therefore if you specified "Show no violating records in alert message", it will only display the number of violations, not the records.

If a severe error occurs which automatically disables the guarded item, that error will not be saved as a Previously Alerted Violation, but can be viewed on the Alert Messages page. Please see the User Guide for more information about severe errors.

**New Violations**

Time Created: 2005-10-05 10:02:23

0 Pre-Defined Rule violations were found (showing all).

- ***GRANTEETYPE*** U ; ***GRANTEE*** DB2ADMIN ; ***GRANTOR*** SYSIBM ; ***TBSPACEID*** 3 ; ***USEAUTH*** G ;

**Previously Alerted Violations (as of last guard cycle)**

There were no previously alerted violations for this policy.

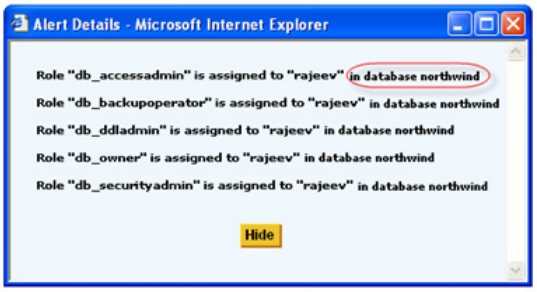
**PDR Violation Details (DB2 example)**

Clicking on the name of the rule will take you to another screen with more detailed violation information.

# Appendix A: Server-Level Assessment, Reporting, and Policy Management for MSSQL Databases

See the *FortiDB MA Installation and Administration Guide* for information on connection to your target database at the server, as well as, the database, level.

## Server-Level PM Monitoring



Role "db_accessadmin" is assigned to "rajeev" in database northwind

Role "db_backupoperator" is assigned to "rajeev" in database northwind

Role "db_ddladmin" is assigned to "rajeev" in database northwind

Role "db_owner" is assigned to "rajeev" in database northwind

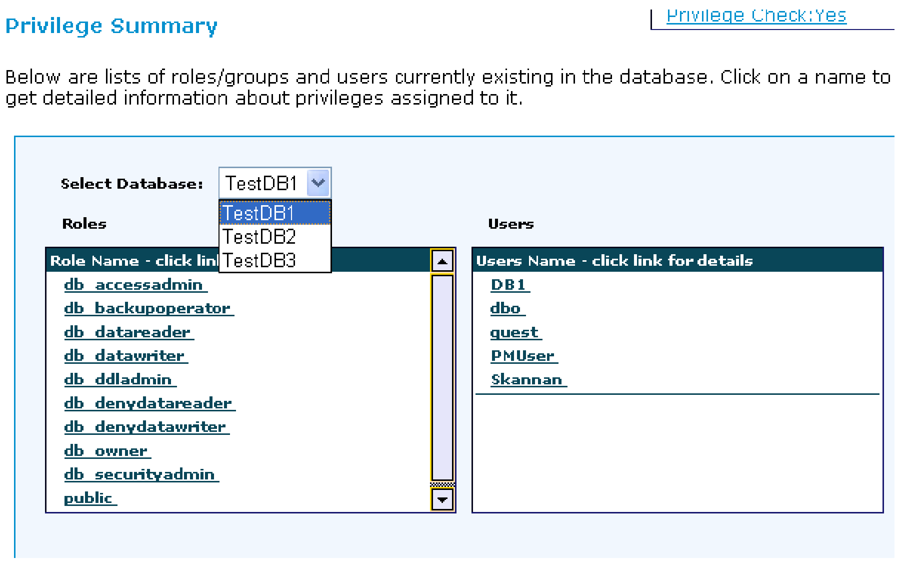
Role "db_securityadmin" is assigned to "rajeev" in database northwind

**Alerts Qualify Violation by Database Name**

When using Server Level monitoring within the Privilege Monitor (PM) module, you can expect alerts to contain information about which database, within that server, was involved in the alert.

**Note:** In the figure above, the `northwind` database was removed from the default list in the `dss.serverlevel.excluded.mssql` list property located in *dssConfig.properties*. You can use this property in order to exclude certain databases from Server Level assessment and monitoring. The default list of databases, which are excluded by this property, are `model,tempdb,pubs,msdb,northwind.`

# Server-Level PM Privilege Summary



**Privilege Summary**

Privilege Check:Yes

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Select Database: TestDB1

- TestDB1
- TestDB2
- TestDB3

**Roles**

| Role Name - click lin |
|---|
| db_accessadmin |
| db_backupoperator |
| db_datareader |
| db_datawriter |
| db_ddladmin |
| db_denydatareader |
| db_denydatawriter |
| db_owner |
| db_securityadmin |
| public |

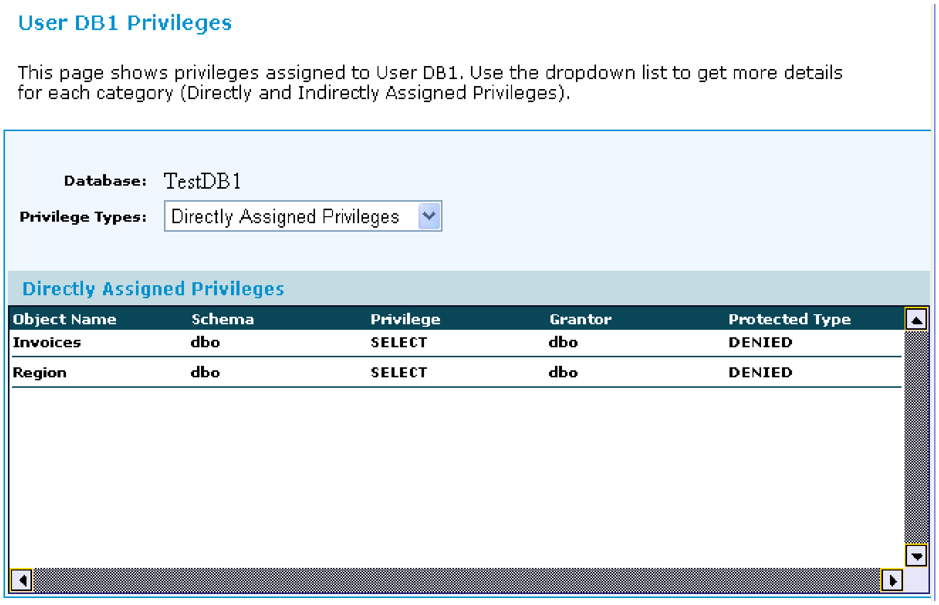
**Users**

| Users Name - click link for details |
|---|
| DB1 |
| dbo |
| guest |
| PMUser |
| Skannan |

**Server-Level Database Selection in Privilege Summary**

Once you have established a Server Level connection, you can then select which database, within that server, you are interested in monitoring.

**Note:** In the figure above, the `master` database was not in the `dss.serverlevel.excluded.mssql` list.



**User DB1 Privileges**

This page shows privileges assigned to User DB1. Use the dropdown list to get more details for each category (Directly and Indirectly Assigned Privileges).

Database: TestDB1

Privilege Types: Directly Assigned Privileges

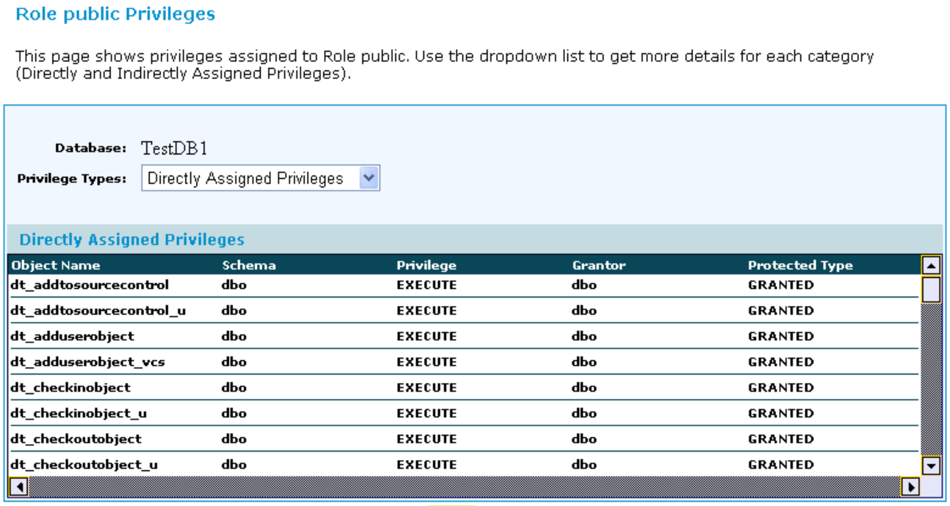
**Directly Assigned Privileges**

| Object Name | Schema | Privilege | Grantor | Protected Type |
|---|---|---|---|---|
| Invoices | dbo | SELECT | dbo | DENIED |
| Region | dbo | SELECT | dbo | DENIED |

**Database Name Listed in Server-Level Role Privileges (MS-SQL Example)**

Once you have selected a particular database within your server, you can get specific privilege information such as Directly Assigned user privileges for that database.

**Note:** In the figure above, the `northwind` database was not in the `dss.serverlevel.excluded.mssql` list.



Role public Privileges

This page shows privileges assigned to Role public. Use the dropdown list to get more details for each category (Directly and Indirectly Assigned Privileges).

Database: TestDB1

Privilege Types: Directly Assigned Privileges

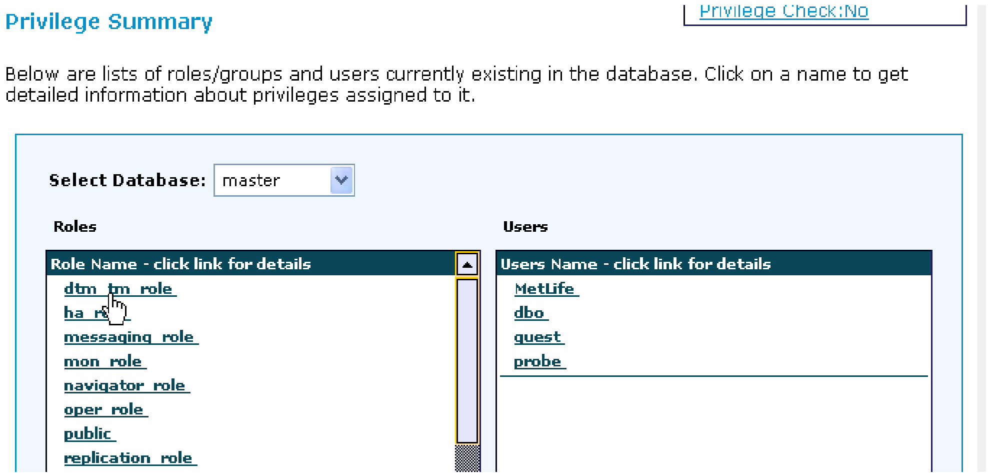
Directly Assigned Privileges

| Object Name | Schema | Privilege | Grantor | Protected Type |
|---|---|---|---|---|
| dt_addtosourcecontrol | dbo | EXECUTE | dbo | GRANTED |
| dt_addtosourcecontrol_u | dbo | EXECUTE | dbo | GRANTED |
| dt_adduserobject | dbo | EXECUTE | dbo | GRANTED |
| dt_adduserobject_vcs | dbo | EXECUTE | dbo | GRANTED |
| dt_checkinobject | dbo | EXECUTE | dbo | GRANTED |
| dt_checkinobject_u | dbo | EXECUTE | dbo | GRANTED |
| dt_checkoutobject | dbo | EXECUTE | dbo | GRANTED |
| dt_checkoutobject_u | dbo | EXECUTE | dbo | GRANTED |

**Database Name Listed in Server-Level Role Privileges**

Once you have selected a particular database within your server, you can get specific privilege information such as Directly Assigned role privileges for that database.

**Note:** In the figure above, the `northwind` database was not in the `dss.serverlevel.excluded.mssql` list.



Privilege Summary

Privilege Check:No

Below are lists of roles/groups and users currently existing in the database. Click on a name to get detailed information about privileges assigned to it.

Select Database: master

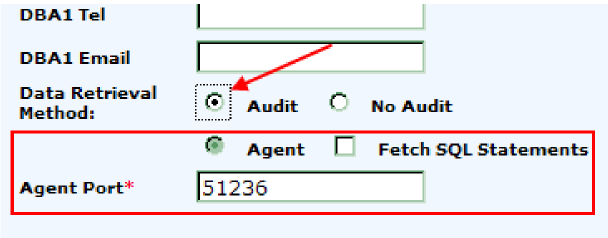
Roles

| Role Name - click link for details |
|---|
| dtm_tm_role |
| ha_role |
| messaging_role |
| mon_role |
| navigator_role |
| oper_role |
| public |
| replication_role |

Users

| Users Name - click link for details |
|---|
| MetLife |
| dbo |
| guest |
| probe |

# Appendix B: DB2-Audit-Based Auditing for DB2 UDB V8



DBA1 Tel

DBA1 Email

Data Retrieval Method: ● Audit ○ No Audit

● Agent □ Fetch SQL Statements

Agent Port* 51236

**Specifying the Use of *DB2 Audit on* Database-Connection Screen**

This feature use of the DB2's *DB2 Audit* functionality, which insures capturing all transactions on the target-database machine, albeit at the expense of requiring an agent.[1]

With the previous FortiDB MA implementation, only a ‘snapshot’ methodology of capturing data for Privilege Monitor was possible. That method only captured at prescribed time intervals, which could lead to missed information if the interval were too large or if the database activity was exceptionally high.

The DB2-Audit-based method, applicable to DB2 V8, overcomes these limitations. In addition, this method allows the reporting of the SQL statements involved in the transaction that caused the alert.

## *Different Data Retrieval Methods*

If you are working with the PM module, you may specify a **Data Retrieval** method of either **Audit** or **No Audit**. The latter, which is the default, invokes the snapshot method.

If you select the **Audit** method, however, FortiDB MA will then use an agent for data collection and provide you with a:

- Checkbox in order to specify whether you want to collect the SQL statements involved. (The default is for this checkbox to be unchecked).
- Text box for the agent's port number (the default is port 51236.)

### Using This Feature

In general, you should follow these steps in order to use the DB2-Audit-based method:

1 Setup and start the DB2-Audit-Based agent on the target-database machine.

[1] Since *db2audit* writes data to a file, the results of which cannot be queried from the JDBC connection, an agent is required in order to send the information back to FortiDB-MA.

2 Define, and **Open and Run,** a database connection, which specifies the **Audit** method of data retrieval.

3 Configure guarded items

4 Get and analyze alerts.

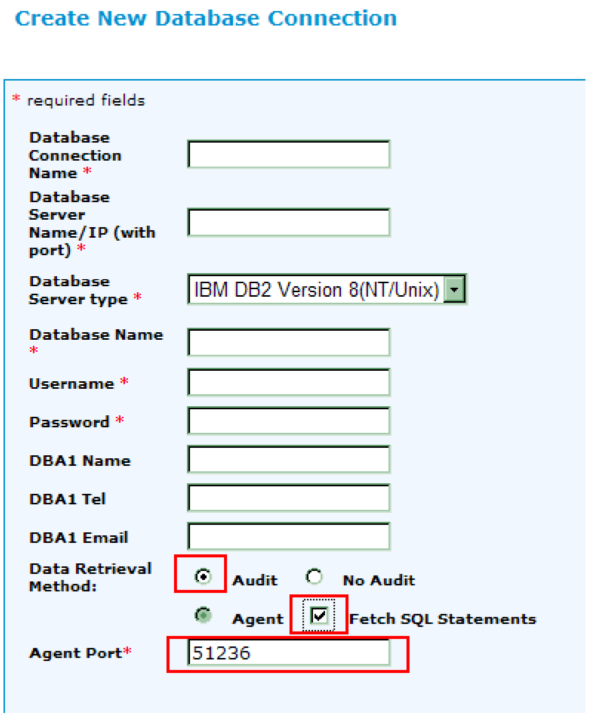
## Setting Up and Starting the Agent

See the Monitoring DB2 Chapter in the *FortiDB MA Administration Guide*.

## DB2 Audit-Based Agent Responsibilities

See the *DB2 Audit*-Based Agent Responsibilities of "Monitoring DB2" in the *FortiDB MA Administration Guide*.

## Define, and Open and Run, a DB2-Audit-Based Connection



Create New Database Connection

* required fields

Database Connection Name *

Database Server Name/IP (with port) *

Database Server type *: IBM DB2 Version 8(NT/Unix)

Database Name *

Username *

Password *

DBA1 Name

DBA1 Tel

DBA1 Email

Data Retrieval Method: ● Audit ○ No Audit

○ Agent ☑ Fetch SQL Statements

Agent Port*: 51236

**Database Connection Page with Audit Retrieval and Fetch SQL Statements both Selected**

Specify the Audit Data Retrieval Method:

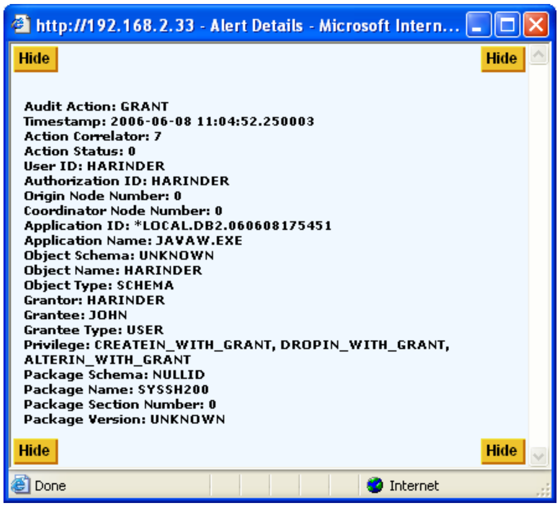
1 Decide whether or not to accept the default **Agent Port.**

2 Decide whether or not you want to capture SQL statements or not.

## Configure Guarded Items

Configure guarded items as you normally would (See Setting Guarded Items)

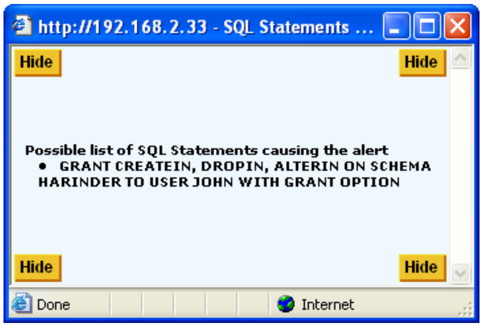
## Get and Analyze Alerts



```
Audit Action: GRANT
Timestamp: 2006-06-08 11:04:52.250003
Action Correlator: 7
Action Status: 0
User ID: HARINDER
Authorization ID: HARINDER
Origin Node Number: 0
Coordinator Node Number: 0
Application ID: *LOCAL.DB2.060608175451
Application Name: JAVAW.EXE
Object Schema: UNKNOWN
Object Name: HARINDER
Object Type: SCHEMA
Grantor: HARINDER
Grantee: JOHN
Grantee Type: USER
Privilege: CREATEIN_WITH_GRANT, DROPIN_WITH_GRANT,
ALTERIN_WITH_GRANT
Package Schema: NULLID
Package Name: SYSSH200
Package Section Number: 0
Package Version: UNKNOWN
```

**PM Alert Generated Using Audit-Based Data Retrieval**

When used with the **Audit Data Retrieval** method, PM generates alerts with the above format.



Possible list of SQL Statements causing the alert

- GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA HARINDER TO USER JOHN WITH GRANT OPTION

**SQL Statements Possibly Causing PM Alert**

If **Fetch SQL Statements** is also checked when creating your database connection, you can analyze a list of possible SQL statements that possibly caused the alert, as shown above.

## Properties

A property, `db2extractdir`, has been introduced in order to help alleviate I/O-contention and/or disk-space problems. This property supports the agent used for DB2-Audit-based auditing used with DB2 UDB V8 target databases. See the *FortiDB MA Administration Guide* for more information.

This property resides in *serverConfigDB28.properties* file which resides on the target-database machine. The default is `/tmp`. You might want to choose another disk location if you encounter an excessively large *db2audit.out* file.

# Index